SyAM Software, Inc.

System Area Manager
V4.0
User Manual

Revision B
January 2009

© 2009 SyAM Software, Inc.
All rights reserved. SyAM Software and the SyAM Software logo are trademarks of SyAM Software, Inc.
All other trademarks are the property of their respective owners.

Information contained in this document is assumed to be accurate at the time of publishing. SyAM Software reserves the right to make changes to the information contained in this document at any time without notice.

For additional information, sales, or technical support, contact SyAM Software

www.syamsoftware.com

Part Number 010150B-EN

Table of Contents

Introduction....7
SyAM Software Modules....8
Compatibility....8
Deployment Options....9
Chapter 1: Installation and Configuration....10
Installation Instructions – Windows....11
Firewall Security....11
Uninstalling SyAM (Windows)....12
Chapter 2: Logging In....13
Browsing to the SyAM Web Server....14
Ending the Session....15
Chapter 3: The SyAM System Area Manager User Interface....16
The SyAM System Area Manager User Interface....17
Interface Layout....17
Dashboard....18
Health Colors....19
Icons....20
Adding Systems to the Management Tree....21
Filter by, Grouping and Sorting Options for the Management Tree....24
Expanding the System Area Manager Tree....26
Chapter 4: License Management....28
License Management....29
Chapter 5: Remote Management....31
Remote Management....32
System State....32
Wake on LAN....33
Remote Console....34
AMT (Intel Active Management Technology)....38
IPMI Event Log....45
IPMI Over LAN....47
Chapter 6: Central Event Logging....49
Central Event Logging....50
Chapter 7: Central Reporting....54
Reporting....55
Chapter 8: Configuring System and Central Alerts....63
System Alert Matrix – System Level Alerting....64
Monitored Sensor Types....65
Physical Sensors....65
Logical Sensors....65
Notification Settings....66
Disabling Notifications....66
Removing a Sensor Instance From the System Alert Matrix....67
Notification Settings – Configuring email alerting....67
Central Alert Matrix....69
Types of monitored events....69
Integration into Enterprise Frameworks....71
Chapter 9: Accessing System Information....72
System Detail Tab....73
Power Management Tab....75
Hardware Detail Tab....78
Network Detail Tab....78
Storage Detail Tab....79
RAID Management....81
Deleting a RAID Set....85
Software Detail Tab....86
Chapter 10: Configuring Platform Event Trap Support....88
Platform Event Traps....89

Configuring System Area Manager to Receive Platform Event Traps....90
Chapter 11: Database Backup/Restore....93
Backing Up the Database....94
Restoring the Database....95
Chapter 12: Contact Details & Glossary....96
Contact Details....97
Glossary....97

Table of Figures

Figure 1: Servers, Desktops and Notebooks being managed individually by each system running the System Client software....9
Figure 2: Servers, Desktops and Notebooks being managed centrally by a system running the System Area Manager software....9
Figure 3: Windows Login Screen....14
Figure 4: Successful Logout....15
Figure 5: SyAM System Area Manager User Interface Layout....17
Figure 6: Header Bar....17
Figure 7: Health State Colors....19
Figure 8: Adding Managed Systems using an IP Address range....21
Figure 9: Status showing 2 systems added....22
Figure 10: Removing a system from the Management Tree....22
Figure 11: Systems Grouped by Location in IP Address Order shown with and without subgrouping....24
Figure 12: Management Tree Filter By, Group By and Sorting Options....25
Figure 13: Examples of the Filter By Option....25
Figure 14: Management Tree – Contracted Groups....26
Figures 15: Management Tree – Expanded Group with contracted Systems....26
Figure 16: Management Tree – Fully expanded Group and Systems....27
Figure 17: License Management Screen – Within Evaluation Period....29
Figure 18: License Management Screen – Entering the Client Access License CAL....30
Figure 19: License Management Screen – With Purchased Client Access License for 20 Desktop/Notebook and 5 Servers....30
Figure 20: Remote Management Option....32
Figure 21: System Status and Wake on LAN Capabilities....32
Figure 22: Wake On LAN (WOL)....33
Figure 23: Remote Console Enabled and Running....34
Figure 24: Remote Console Login....35
Figure 25: Remote Console – Managing a remote System....35
Figure 26: Remote Console File Transfer....36
Figure 27: Remote Console – Clipboard....37
Figure 28: Remote Console – Disconnect....37
Figure 29: AMT Login Tab....38
Figure 30: Launching the AMT Console....38
Figure 31: Establish AMT Connection....39
Figure 32: AMT Remote Control....40
Figure 33: Serial Over LAN (In Use showing BIOS Re-configuration)....40
Figure 34: IDE-R (Configured to boot off CD-Rom)....41
Figure 35: IDE-R (In Use showing remote boot off CD-Rom)....42
Figure 36: AMT System Defense (Establish AMT Connection)....43
Figure 37: Download AMT Policies....43
Figure 38: AMT System Defense Policies....44
Figure 39: IPMI Event Log....45
Figure 40: IPMI Event Log Retrieval....46
Figure 41: IPMI Over LAN – Enter details for accessing the BMC....47
Figure 42: IPMI Over LAN – Details applied....47
Figure 43: IPMI Over LAN – Connected....48
Figure 44: Event Log Filtering Options....50
Figure 45: Viewing the HTML Event Log on screen....52
Figure 46: Viewing the Process Snap Shot for a Memory Utilization Event....52
Figure 47: Deleting Events....53
Figure 48: System Area Manager Reports....55
Figure 49: Application Summary Report....56
Figure 50: Asset List Report....59
Figure 51: Asset Summary Report....60
Figure 52: Operating System Summary Report....61

Figure 53: Power Audit Report....62
Figure 54: System Alert Matrix....64
Figure 55: Setting Category and Instance-Level Notifications....66
Figure 56: Entering Notification Information....68
Figure 57: Central Alert Matrix....70
Figure 58: System Detail Tab....73
Figure 59: System Detail Tab Continued....73
Figure 60: Power Management Tab....75
Figure 61: Hardware Detail Tab....78
Figure 62: Network Detail Tab....79
Figure 63: Storage Detail Tab....79
Figure 64: Storage Details – Managed RAID Controllers....81
Figure 65: RAID Controller Details Screen....82
Figure 66: Physical Drives – Choosing drives for the Array....83
Figure 67: Available Array - Configuring the RAID Set....83
Figure 68: RAID Set Details – Information on Configured RAID Set....84
Figure 69: Removing a Hot Spare drive....84
Figure 70: RAID Set Details – Deleting a RAID set....85
Figure 71: Software Detail Tab....86
Figure 72: End the Process....86
Figure 73: Confirm to End the Process....86
Figure 74: Starting a Service....87
Figure 75: Confirm to Start the Service 87
Figure 76: Stopping a Service....87
Figure 77: Confirm to Stop the Service 87
Figure 78: Example of a PET email alert....89
Figure 79: Example of PET information in the Event Log....89

Introduction

SyAM Software provides a comprehensive, simple to use set of system management products for servers, desktops and notebooks. Each product has features specific to their relevant system's capabilities and functions, as well as a large number of common features. Their user interfaces are identical.
The products enable several IT benefits. Among them are predictive alerting to pending failures, system configuration, unattended monitoring and alerting, remote management, and reporting. The products dynamically discover the hardware and software operating environment, and manage all physical environmental sensors available and operating system resources. Users can view them and be alerted if they exceed their thresholds.

There are two levels of system management. System Client software provides a single system view. System Area Manager software provides a unified view of all of your systems, and also provides more comprehensive features.

The System Client management products are:

- *Server System Client*
- *Desktop System Client*
- *Notebook System Client*

The Central Management product is:

- *System Area Manager*

This user manual describes the System Area Manager software. The following sections will describe the product functionality of the System Area Manager software itself, and also explain how managing other systems via a System Area Manager unlocks features in those systems.

SyAM Software Modules

System Area Manager software contains two products;

- **System Area Manager – Server –** This software provides the ability to manage Servers, Desktops and Notebook platforms running the System Client Software.
- **System Area Manager – Desktop** - This software provides the ability to manage Desktops and Notebook platforms running the System Client Software.

These products can be installed on any Intel architecture x86/x64 platform running one of the supported operating systems.

Compatibility

Operating System	***System Area Manager - Server***	***System Area Manager - Desktop***
Windows 2008 Server	■	
Windows 2003 Server	■	
Windows Vista Business	■	■
Windows XP Professional	■	■

System Requirements

- 1GB Disk space
- 2GB Memory

Browser Requirements

- Internet Explorer 6+ (Service Pack 1)
- Mozilla Firefox (V2.0.x or above)

Deployment Options

Administrators use Internet Explorer or Firefox to browse to the System Client Interface on the system being managed
Server running Server System Client
Desktop running Desktop System Client
Notebook running Notebook System Client
System Client Agents send event notification messages to administrators via email

Figure 1: Servers, Desktops and Notebooks being managed individually by each system running the System Client software.

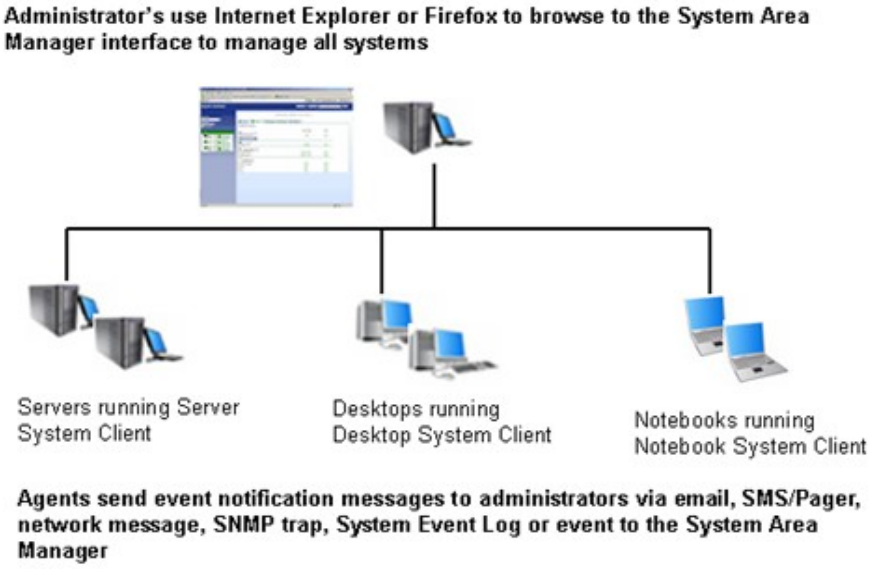

Administrator's use Internet Explorer or Firefox to browse to the System Area Manager interface to manage all systems
Servers running Server System Client
Desktops running Desktop System Client
Notebooks running Notebook System Client
Agents send event notification messages to administrators via email, SMS/Pager, network message, SNMP trap, System Event Log or event to the System Area Manager

Figure 2: Servers, Desktops and Notebooks being managed centrally by a system running the System Area Manager software.

Chapter 1: Installation and Configuration

This chapter provides step-by-step installation and configuration instructions for SyAM System Area Manager software on Windows and Linux Operating System Platforms

It is recommended that you print off the quick start guide before installing the software too. This simple document will step you through installation and email configuration in a few minutes.

Installation Instructions – Windows

1. Either load the SyAM Software CD and from the menu choose the product version you wish to install, or double click the downloaded SyAM executable. Then just follow the Install Wizard instructions.
2. Choose the language of the user interface.
3. Choose the destination folder (This can not contain any spaces in the name)
4. Do not change the RMI port default value of 10999 unless you know that port number is already in use
5. To enable security through 128-bit data encryption from the SyAM Server Web Server to the browser, choose the SSL option. (default=No)
6. After the installation has finished, the SyAM services will start and dynamically discover and configure your system's monitoring environment.

Firewall Security

The following ports must be opened if you are using a firewall on your Linux system. They are automatically opened on Windows 2003 and XP Pro systems during the installation.

- 3894 – Used for Agent management service
- 3895 – Used for Central management service
- 3930 – Used for Web server service
- 5800 – Used for Remote Console access from System Area Manager
- 5900 – Used for Remote Console access from System Area Manager
- 58900 – AMT SOL – Session #1
- 58901 – AMT SOL – Session #2
- 58902 – AMT SOL – Session #3

Uninstalling SyAM (Windows)

To remove the SyAM software from the windows system:

1. On the start menu, select <Settings> <Control Panel> <Add/Remove Programs>
2. Highlight SyAM and select <Remove>. You will be prompted to confirm this action.
3. Following removal, if SyAM software is to be reinstalled then a system restart is required.

Chapter 2: Logging In

This chapter provides details on logging into the SyAM User Interface

Browsing to the SyAM Web Server

Open a supported web browser on any system and access the SyAM user interface on any system with the System Area Manager installed. Then enter:

http://IPADDRESS or the MACHINENAME:3930

Example http://192.168.1.19:3930

Example http://FILESEVER:3930

If you enabled SSL during installation, you are required to type "https" instead of "http":

Example: https://IPADDRESS or https://MACHINENAME:3930

This will bring you to the log in screen.

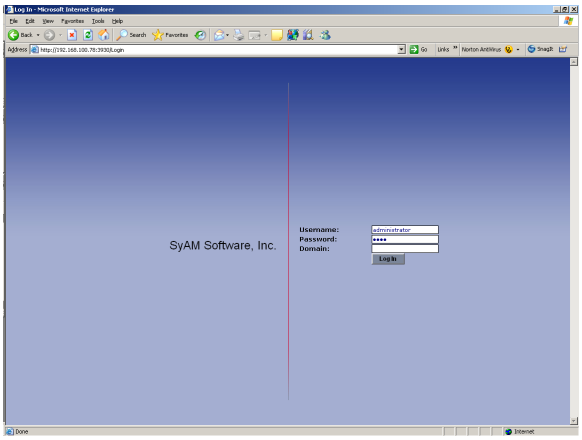


Figure 3: Windows Login Screen

The SyAM web server does not maintain its own separate set of users and passwords. It requests the operating system to log you in, so uses the accounts that are already in place on your system. To login you must satisfy the following conditions:

For Standalone systems (not in a Windows Domain)

- The User name and Password must be valid on the system you are logging into.
- The User must have Administrator rights on the system.

For systems within a Windows Domain

- The User name and Password must be valid in the Domain.
- The User must have "Domain Admin" rights within the Windows Domain
- A Valid Domain Name for the system must be entered in the Domain field.

Ending the Session

When you have completed your management session, choose the Log Out button on the main header bar. Successful logout returns you to the login screen:

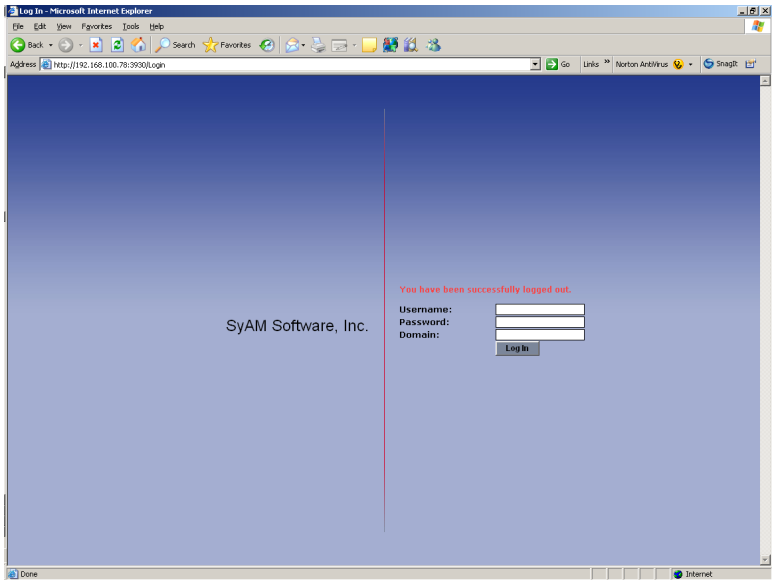


Figure 4: Successful Logout

For added security you will be logged out automatically after 30 minutes of inactivity. A message box will appear on screen if you are using Internet Explorer to let you know that you need to log back in. If you are using a Firefox browser you will be logged out and put back to the login screen.

Chapter 3: The SyAM System Area Manager User Interface

This chapter describes how to use the SyAM System Area Manager software. It also points out the enhancements made to the systems running the System Client software when those systems are managed centrally.

The SyAM System Area Manager User Interface

SyAM System Area Manager software provides administrators with the ability to manage a set of systems from a single user interface.

Interface Layout

The structure of the interface is identical whether you are using System Area Manager Server or Desktop. All of the systems being managed are represented in the tree on the left hand side. Detailed information about a specific system being accessed in presented on the main right hand side.

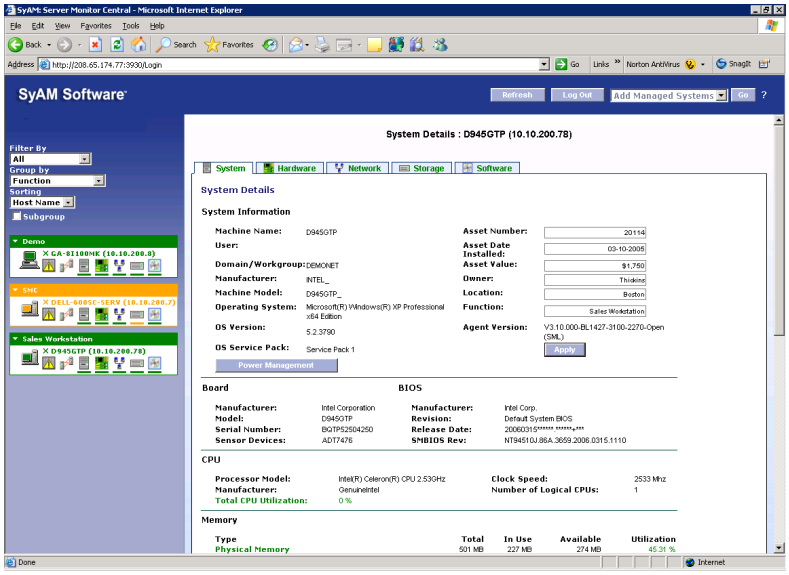


Figure 5: SyAM System Area Manager User Interface Layout

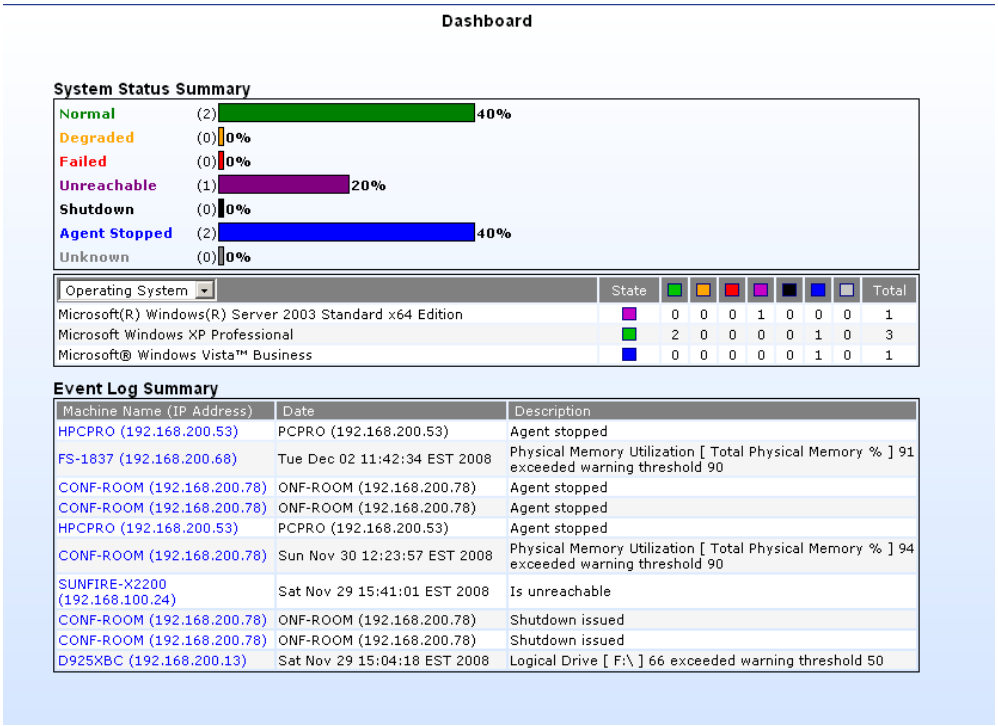
Header Bar

The header bar has three function buttons – Refresh, Log out and Online Help and a Drop Down menu for the central management functions – Dashboard, Add Managed Systems, Central Alert Matrix, Event Log, Report, License Management, and Version

Figure 6: Header Bar

Dashboard

The Dashboard provides the user with a chart showing the state of their managed systems. It displays the systems by the chosen grouping and the last 10 events that have occurred.


Dashboard
System Status Summary
Normal (2) 40%
Degraded (0) 0%
Failed (0) 0%
Unreachable (1) 20%
Shutdown (0) 0%
Agent Stopped (2) 40%
Unknown (0) 0%
Operating System
State
Total
Microsoft(R) Windows(R) Server 2003 Standard x64 Edition 0 0 0 1 0 0 0 1
Microsoft Windows XP Professional 2 0 0 0 0 1 0 3
Microsoft® Windows Vista™ Business 0 0 0 0 0 1 0 1
Event Log Summary
Machine Name (IP Address) | Date | Description
HPCPRO (192.168.200.53) | PCPRO (192.168.200.53) | Agent stopped
FS-1837 (192.168.200.68) | Tue Dec 02 11:42:34 EST 2008 | Physical Memory Utilization [Total Physical Memory %] 91 exceeded warning threshold 90
CONF-ROOM (192.168.200.78) | ONF-ROOM (192.168.200.78) | Agent stopped
CONF-ROOM (192.168.200.78) | ONF-ROOM (192.168.200.78) | Agent stopped
HPCPRO (192.168.200.53) | PCPRO (192.168.200.53) | Agent stopped
CONF-ROOM (192.168.200.78) | Sun Nov 30 12:23:57 EST 2008 | Physical Memory Utilization [Total Physical Memory %] 94 exceeded warning threshold 90
SUNFIRE-X2200 (192.168.100.24) | Sat Nov 29 15:41:01 EST 2008 | Is unreachable
CONF-ROOM (192.168.200.78) | ONF-ROOM (192.168.200.78) | Shutdown issued
CONF-ROOM (192.168.200.78) | ONF-ROOM (192.168.200.78) | Shutdown issued
D925XBC (192.168.200.13) | Sat Nov 29 15:04:18 EST 2008 | Logical Drive [F:\ ] 66 exceeded warning threshold 50

You can change the view of the system status summary by clicking on the down arrow and selecting the appropriate logical group.

To sort the management tree to display only a specific set of systems click on the status chart or the column and it will refresh the management tree with that filter by status.

Within the Event Log Summary you can click on the Machine Name and the page will change to that systems information.

The Dashboard will automatically refresh every minute.

Health Colors

In order to quickly identify and correct system problems, SyAM software uses a consistent color scheme to represent the health and functionality of systems and their components. These colors can be seen in every level of monitoring, from the instance of the component to the component category and section.. The health of each monitored system is updated on a regular interval. Any change in the status of the system will cause a change in the health color. The health color will remain in the changed state until the issue is resolved.

	Green = Fully Functional
	Amber = Warning
	Red = Critical
	Grey = System state pending, currently unknown
	Purple = System is no longer responding
	Blue = Agent service has been manually shutdown
	Black = System has been shutdown
	Cyan = System has expired Central Management License Key

Figure 7: Health State Colors

Icons

There are three icons that represent the type of SyAM software running on the managed system.

Server System Client/System Area Manager

Desktop System Client/System Area Manager

Notebook System Client

Adding Systems to the Management Tree

Systems must be added to the Management Tree before they can be managed centrally through the System Area Manager software.

You can only add systems that are running SyAM software, and may only add those systems up to the limit set by your license key.

Once a system is added it will automatically unlock the System Client software running on that system, which will now send event messages to the System Area Manager software.

To add a system or discover systems to be added to the System Area Manager choose Add Managed Systems from the Drop down menu on the header bar.

1. Enter the IP Addresses in the **From** and **To** fields

   To add a single system enter the same IP address in the **From** and **To** fields
   To discover systems across a network address range, enter the lower IP Address in the **From** field and the higher IP address in the **To** field.

   It is recommended to keep the IP address range "dense". The longest wait times occur when trying to sample IP addresses that are not in use.

2. Enter the **Location** and **Function** that is to be applied to the discovered systems (These values are used in grouping and sorting of the tree.)
3. Press the **Apply** button
4. You will now see a status of the addition scan saying how many systems have been scanned out of the total to be scanned
5. You can cancel the scanning by pressing the **Cancel** button
6. Once discovery has been completed the **Status** will show the amount of systems successfully added

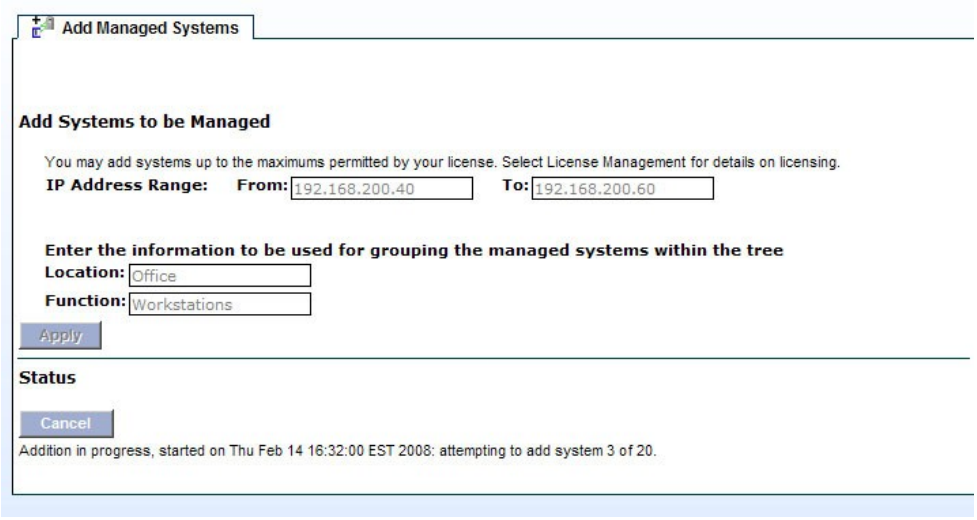

Add Managed Systems
Add Systems to be Managed
You may add systems up to the maximums permitted by your license. Select License Management for details on licensing.
IP Address Range:
From: 192.168.200.40
To: 192.168.200.60
Enter the information to be used for grouping the managed systems within the tree
Location: Office
Function: Workstations
Apply
Status
Cancel
Addition in progress, started on Thu Feb 14 16:32:00 EST 2008: attempting to add system 3 of 20.

Figure 8: Adding Managed Systems using an IP Address range

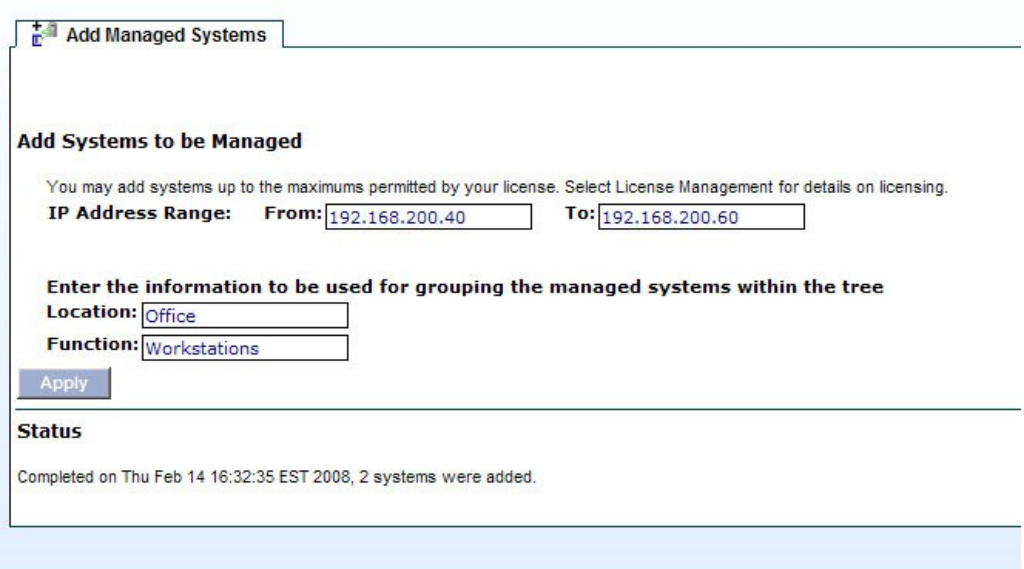

Add Managed Systems
Add Systems to be Managed
You may add systems up to the maximums permitted by your license. Select License Management for details on licensing.
IP Address Range: From: 192.168.200.40 To: 192.168.200.60
Enter the information to be used for grouping the managed systems within the tree
Location: Office
Function: Workstations
Apply
Status
Completed on Thu Feb 14 16:32:35 EST 2008, 2 systems were added.

Figure 9: Status showing 2 systems added

Changing to which System Area Manager the system reports

Remove the system from the first System Area Manager tree to stop the system from reporting. Once this is done, add the system to the second System Area Manager tree by following the instructions "Add Managed System"

Removing Managed Systems

If you wish to remove a managed system from the System Area Manager Tree:

- Click on the <X> next to the name of the system
- You will be prompted to confirm the deletion of this system

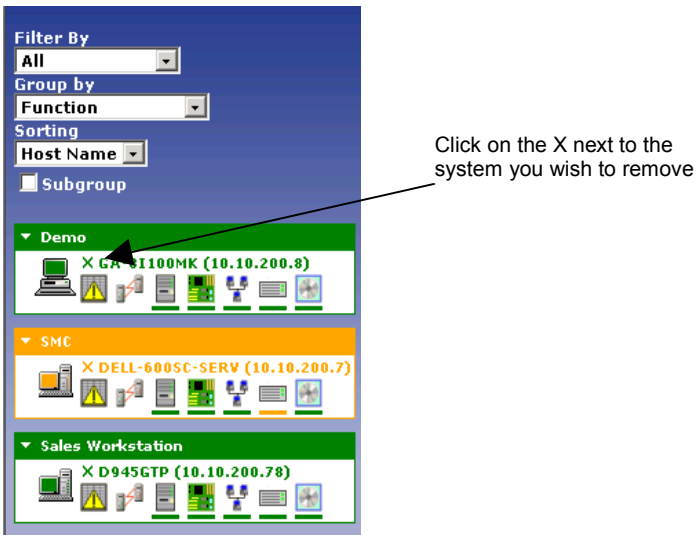


Figure 10: Removing a system from the Management Tree

Once a system has been removed from the Management Tree the System Client software will go back to email alerting only and will not report its events to the System Area Manager.

The system you removed is still being monitored for health by the management agent on that system, which will alert via email to any issues it discovers. You may add the system back into the System Area Manager tree at any time.

If you wish to completely disable this monitoring on the removed system, uninstall the software on that system.

Filter by, Grouping and Sorting Options for the Management Tree

Systems listed on the Management Tree are filtered by showing all health states and grouped by operating system and sorted by machine name by default. By using the Filter By drop down menu, administrators can choose to only show a certain health state, helping the administrator to narrow down their view to only systems with a certain health state.

By using the Group By drop down menu, administrators can choose to view groups of systems by location or by function, helping the administrator to narrow down issues in environments with large numbers of systems.

By using the Sorting drop down menu, administrators can select to view the systems within the groups by Machine Name or IP Address within the groups; this reverses the display order to IP Address/Machine name for IP sorting order and Machine Name/IP Address for Machine Name sorting order.

The administrator can modify the **Location** and **Function** fields in the System screen for each managed system. If this information has not been specified for some managed systems, the grouping function will display the systems as “Ungrouped” as the name for the location or function.

If Server, Desktops and Notebooks are being monitored the Subgroup option will be displayed.

By clicking on the Subgroup check box, the tree will be shown where the sorting within the chosen group will show the all Servers first, then Desktops and then Notebooks.

If Subgroup is not chosen then the sorting will be in the chosen order without any sub grouping of server/desktop/notebook.

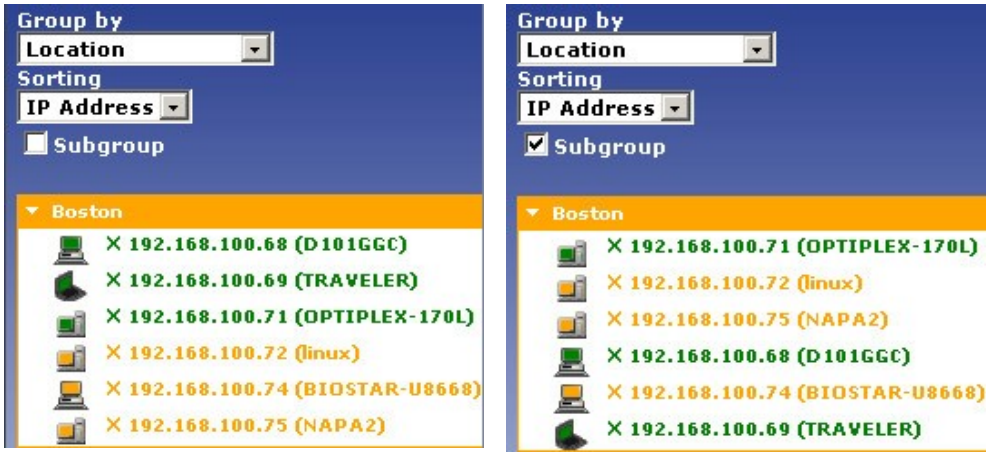


Figure 11: Systems Grouped by Location in IP Address Order shown with and without subgrouping

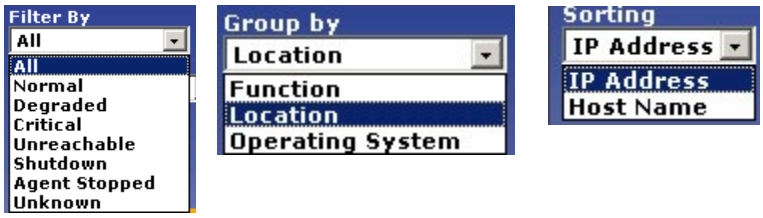


Figure 12: Management Tree Filter By, Group By and Sorting Options

The administrator can use the Filter By to choose to only show systems at a specific Health State.

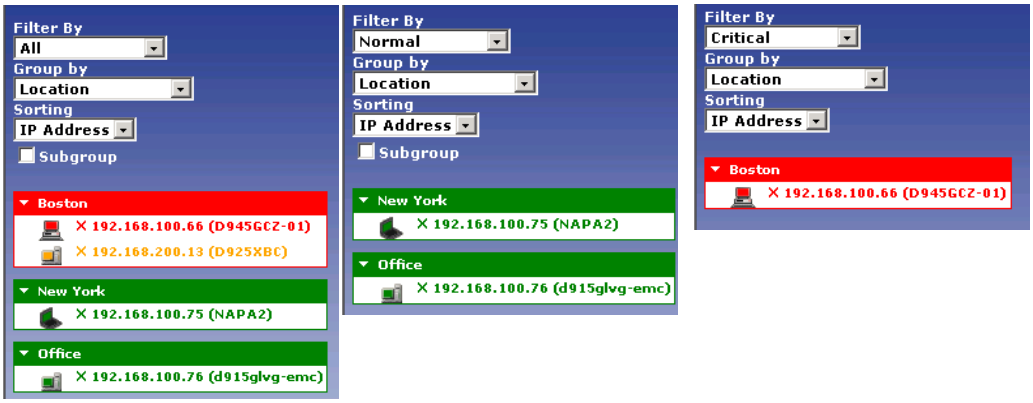


Figure 13: Examples of the Filter By Option

Expanding the System Area Manager Tree

System Area Manager provides administrators with an overall view of managed system, and the capability to drill down tzo each system and individual components.

Click on the name of the operating system, function, or location to expand the list of systems in each group. The names and IP addresses of each system will be displayed in the left hand window.

Figure 14: Management Tree – Contracted Groups

Figures 15: Management Tree – Expanded Group with contracted Systems

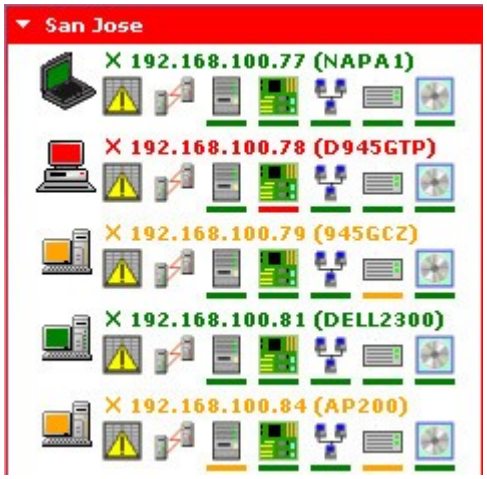


Figure 16: Management Tree – Fully expanded Group and Systems

Tree Icons

	System Alert Matrix – Provides access to the thresholds, sample,reset periods and notification options for all of the monitored hardware and software sensors within the system
	Remote Management – Provides access to the remote functions, Shutdown, Restart, Wake on LAN and Remote Console which provides the administrator full access to the remote systems keyboard, mouse and screen. IPMI – Provides access to IPMI Event log data while system is running, also provides IPMI Over LAN Power Management and Event Log access out of band (system may be powered off).
	System – Provides system board, memory, CPU, slot, display, port information and status of the CPU and Memory utilization being monitored, in addition memory error information is displayed.
	Hardware – Provides sensor information and current status on physical sensors being monitored within the system
	Network – Provides network adapter configuration information and performance for all configured adapters within the system
	Storage – Provides physical storage device, storage controller, logical device information and health status for the storage devices and managed RAID controllers.
	Software – Provides information on OS services, processes, and installed applications. Also provides remote and process management.

Chapter 4: License Management

This chapter describes how to process License Keys for continued use of System Area Manager after the evaluation period has expired, and to increase in the number of systems the System Area Manager can manage.

License Management

System Area Manager provides the ability to manage up to 2000 systems from a single user interface. The amount of systems that can be managed is controlled through a Client Access License (CAL).

The software ships with a 15 day evaluation license that enables full System Area Manager capabilities to a limited number of systems.

Note: If the evaluation period expires, almost all of the System Area Manager functions will be disabled. However you will still be able to access the License Management screen and enter the Client Access License number.

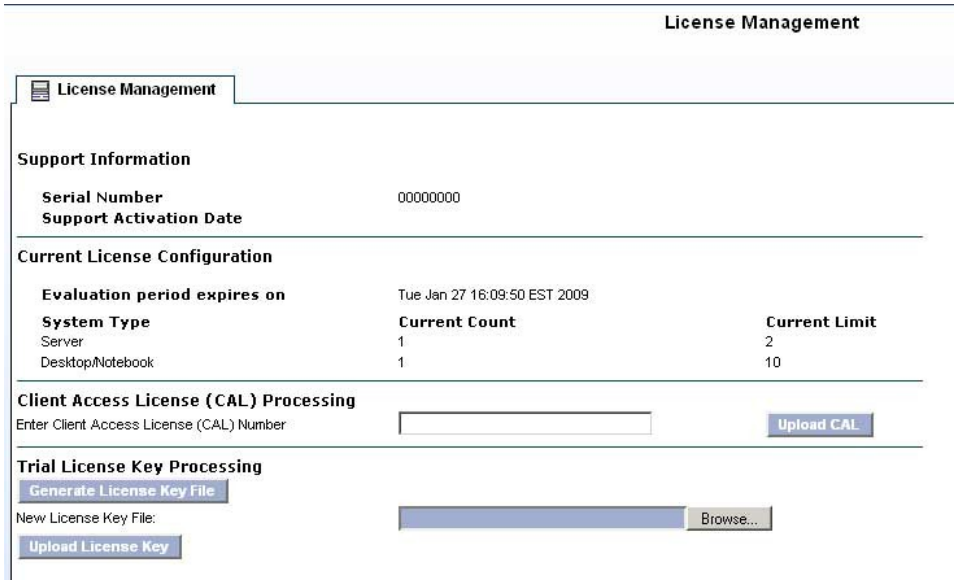


Figure 17: License Management Screen – Within Evaluation Period

To unlock the ability to manage more systems or for continued use after the evaluation period has expired a Client Access License must be purchased.

To access the License Management Screen you choose it from the Drop Down menu on the header bar.

1. Open up the License Management screen on the System Area Manager that you wish to enter the Client Access License for.
2. Enter the Client Access License number into the box and press Upload CAL.
3. The System Area Manager will process the Client Access License and the current limits will be increased to the limits that you purchased.
4. If this is the first time you purchased a key for this System Area Manager you will be provided with a support Serial Number and when Support Activation Date.

Figure 18: License Management Screen – Entering the Client Access License CAL

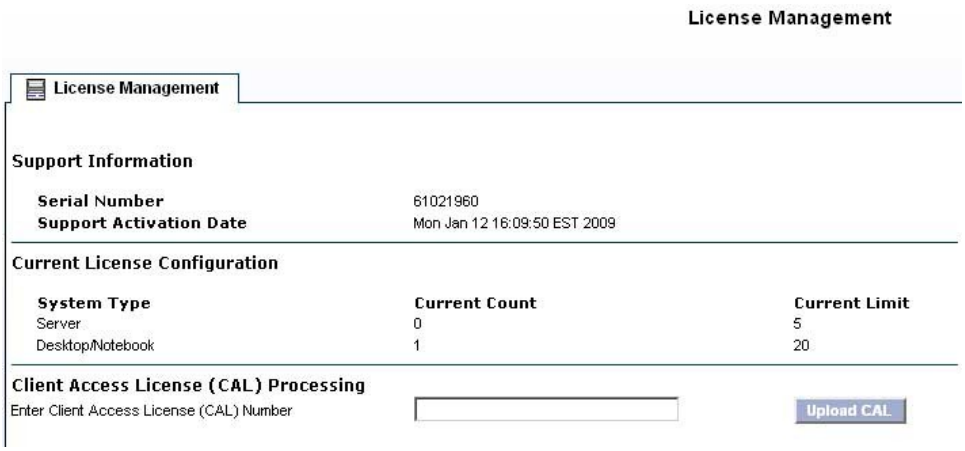


Figure 19: License Management Screen – With Purchased Client Access License for 20 Desktop/Notebook and 5 Servers

Chapter 5: Remote Management

This chapter describes how to use the Remote Management capabilities within the System Area Manager User Interface.

Remote Management

System Area Manager provides remote management functions for its managed systems, including Wake on LAN, Shutdown, Restart, Remote Console and for AMT enabled system it provides, AMT power Management, for IPMI enabled systems it provides IPMI Event Log and IPMI Over LAN for IPMI.

To access remote management; choose this option from the listed system on the System Area Manager tree.

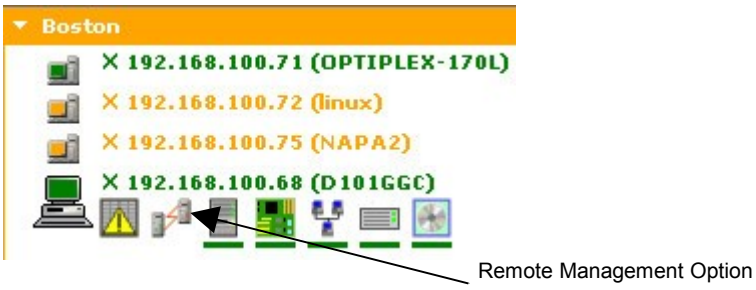


Figure 20: Remote Management Option

System State

The system state screen contains information on the current condition of the selected system, using the same health color scheme. System Area Manager remote management provides Shutdown / Restart, Wake on LAN and Remote Console management options. In order to use the Shutdown, Restart, and Remote Console management options, the System Client software must be running.

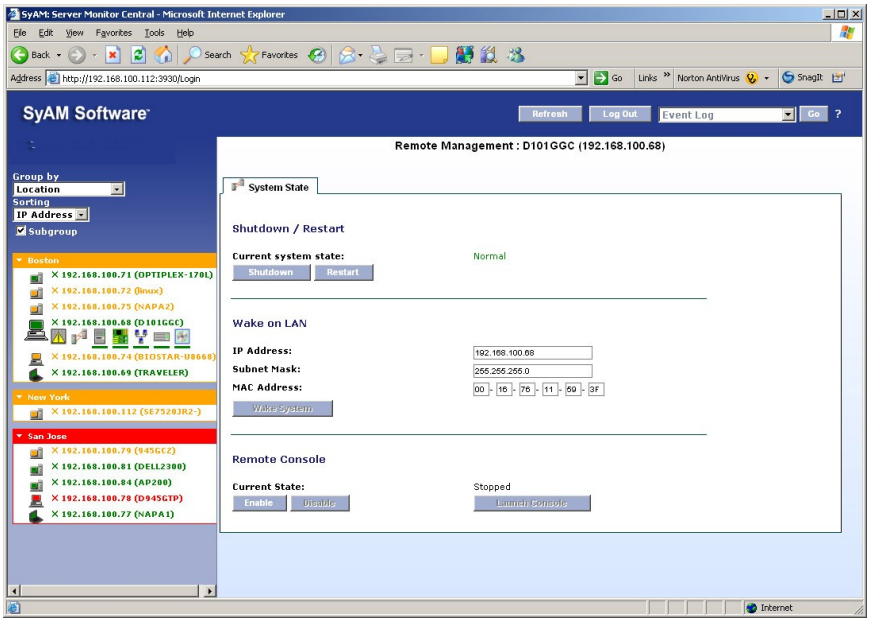


Figure 21: System Status and Wake on LAN Capabilities

To shutdown or restart the system, the system must be in Normal, Warning or Critical health states.

- To shutdown a system, click <shutdown>
- You will be prompted to confirm this action
- To restart a system, click <restart>

- You will be prompted to confirm this action

Wake on LAN

Wake on LAN capability allows central administrators to power up a WOL enabled managed system. In order for Wake on LAN to function properly, the administrator must have enabled this capability within the managed system's BIOS.

To wake a system, the system must be in the Shutdown health state.

- The IP address and MAC address of the system is automatically populated by the System Area Manager.
- Click the <wake system> button to wake the system remotely

The administrator can change the MAC Address and IP Address of the network connection to be notified with the WOL command. Use this when the managed system is reporting to the System Area Manager on the non WOL-enabled network adapter. Note that System Area Manager will need to be able to access the WOL enabled Network adapter for this function to work.

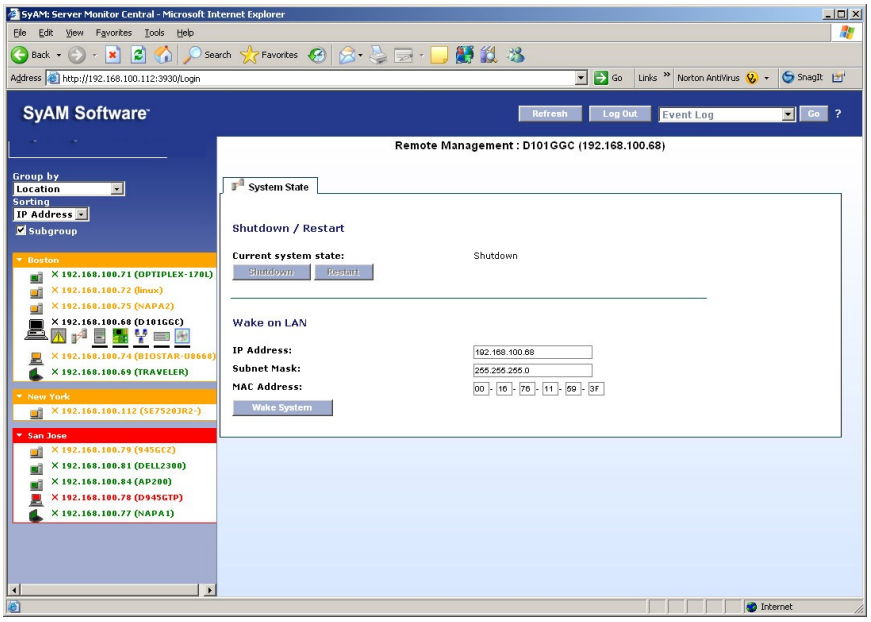


Figure 22: Wake On LAN (WOL)

Remote Console

Remote Console provides the capability of taking control of a managed systems local screen, keyboard and mouse directly through the Server/Desktop System Client interface.

To access the Remote Console, select the system from the Management Tree, click on the Remote Management icon, which opens the remote management screen. The bottom section of the screen shows the Remote Console status and Enable/Disable and Launch Console buttons.

The status must be running if you wish to launch the console.

Click on the Enable button to start the service on the remote managed system.
Click on the Disable button to stop the service on the remote managed system.
Click on the Launch Console button to establish a remote console session.

We recommend you disable the remote console feature (which stops the software from running) after each use; however the software will automatically be stopped once the managed system is rebooted.

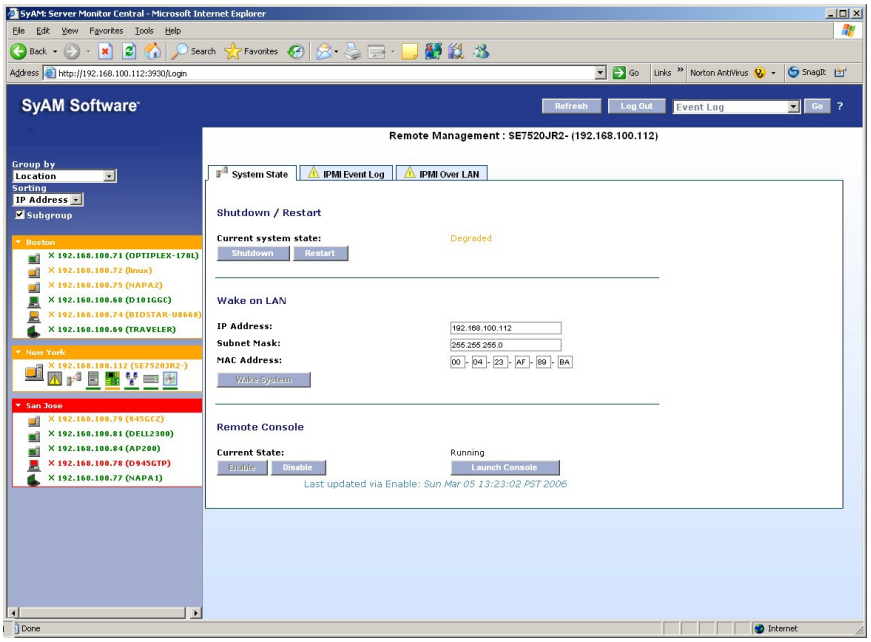


Figure 23: Remote Console Enabled and Running

Once you launch the console enter the password (Windows Default is 1234) and this console session now provides access to the remote system.

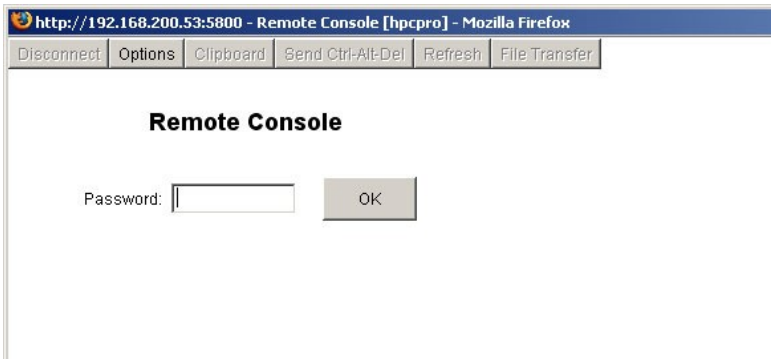


Figure 24: Remote Console Login

Now the windows represents the screen of the managed system, once finished click on Disconnect and close the window.

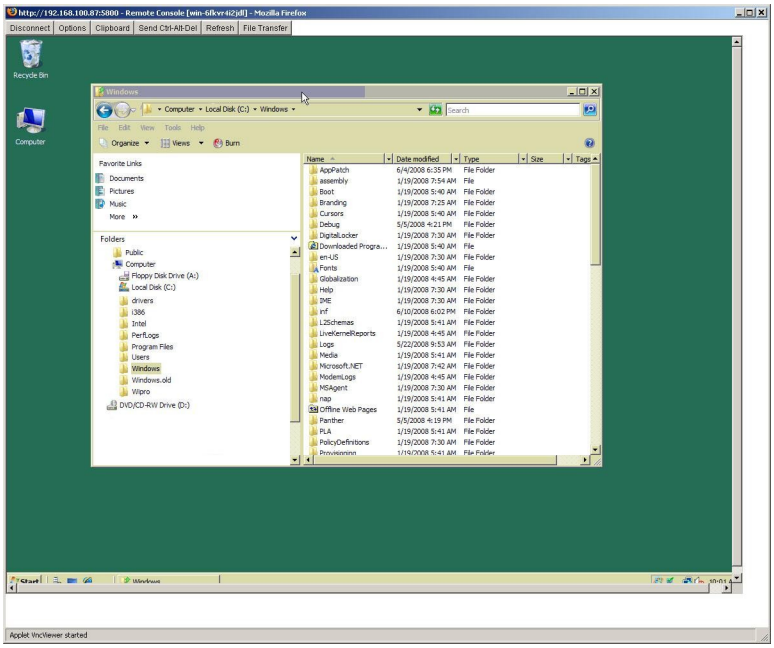


Figure 25: Remote Console – Managing a remote System

For Windows system the Remote Console function has a File Transfer Option. To transfer files to and from the system you are accessing via Remote Console click on the File Transfer option at the top. This will open up a file transfer window.

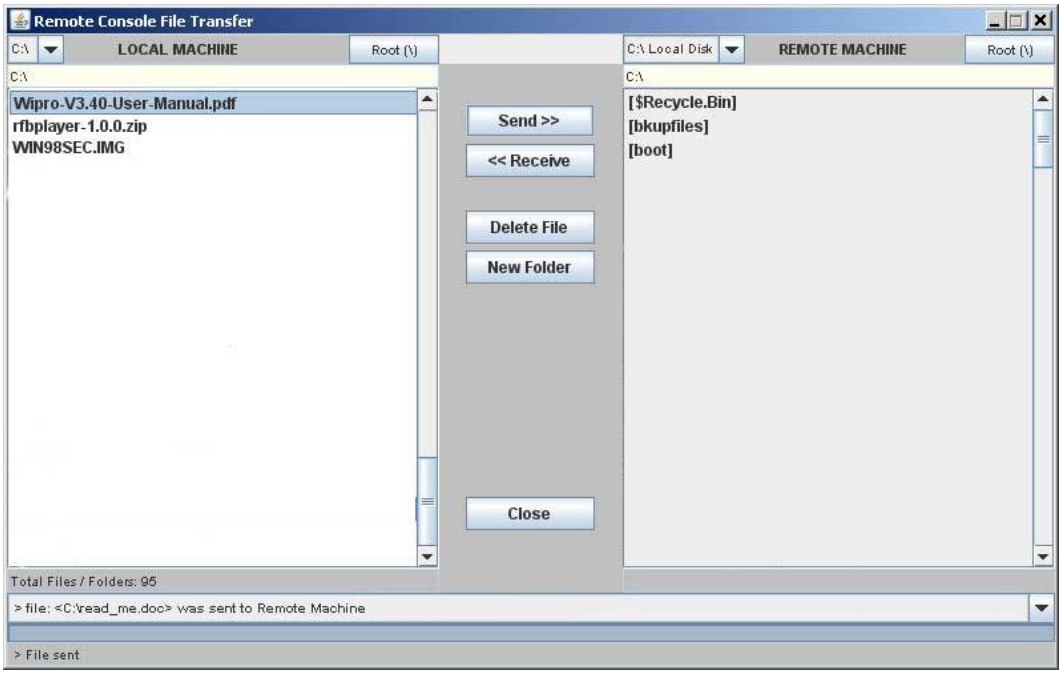


Figure 26: Remote Console File Transfer

Navigate to the file on the Local or Remote Machine and press the Send or Receive button.

Receive to transfer the file from the Remote Machine to the Machine you are browsing from

Send to transfer the file from the Machine you are browsing from to the Remote Machine

Changing the Default Password

To change the password from the default:

On Windows:

Please use the Management Utility software version 4.30 or above

On Linux: Default password is 12345678

cd to the top-level directory where the System Area Manager software was installed.
From there:

```
cd system_monitor/remote_console
./vncpassword
```

You will be prompted to enter and then confirm the new password.

Using the Clipboard

To copy information from the managed system to the local System Area Manager, select the information to copy and use the edit/copy command, then click on the Clipboard button at the top menu, then paste the information to the clipboard. Now select the information in the clipboard and copy/paste it into a file on the local system.

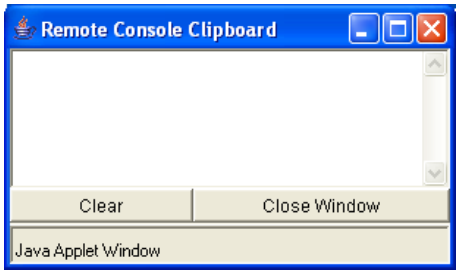


Figure 27: Remote Console – Clipboard

Ending the Remote Console Session

To end the Remote Console session, click the disconnect button at the top menu. Settings.

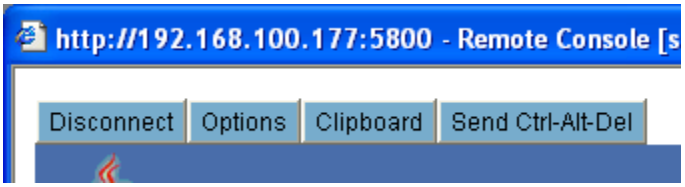


Figure 28: Remote Console – Disconnect

AMT (Intel Active Management Technology)

The AMT Tab will only appear if the system running the System Client is identified as having Intel AMT technology onboard.

Server/Desktop/Notebook System Client can provide power management and AMT Console access when the system is in either an operating system-present or -absent state.

Please check www.syamsoftware.com/vpro for validated AMT configurations

You must first configure the AMT Port IP address and Password using the vendor provided utilities before you can utilize this AMT feature.

Enter the user name, password and IP address of the AMT port for the managed system, then click on the apply button to save this data.

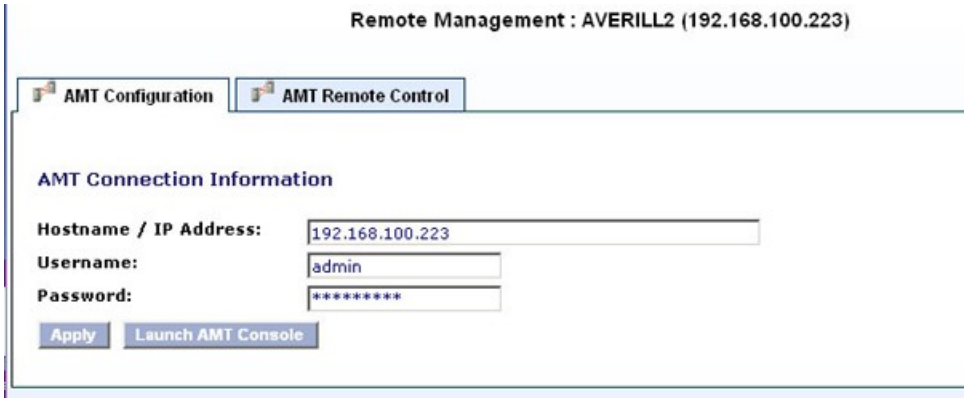


Figure 29: AMT Login Tab

Click on Launch AMT Console to open up a new browser window and login directly into the embedded AMT web server.

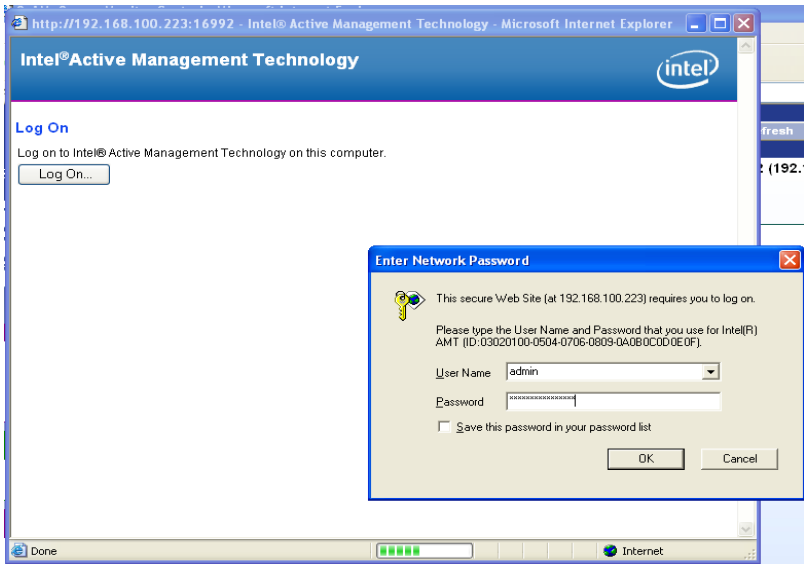

http://192.168.100.223:16992 - Intel® Active Management Technology - Microsoft Internet Explorer
Intel®Active Management Technology
intel
Log On
Log on to Intel® Active Management Technology on this computer.
Log On...
Enter Network Password
This secure Web Site (at 192.168.100.223) requires you to log on.
Please type the User Name and Password that you use for Intel(R) AMT (ID:03020100-0504-0706-0809-0A0B0C0D0E0F).
User Name
admin
Password
Save this password in your password list
OK
Cancel
Done
Internet

Figure 30: Launching the AMT Console

Once you have saved the User name, password and IP Address you can click on the Establish AMT Connection button under the AMT Remote Control Tab to access the managed system's AMT over the LAN.

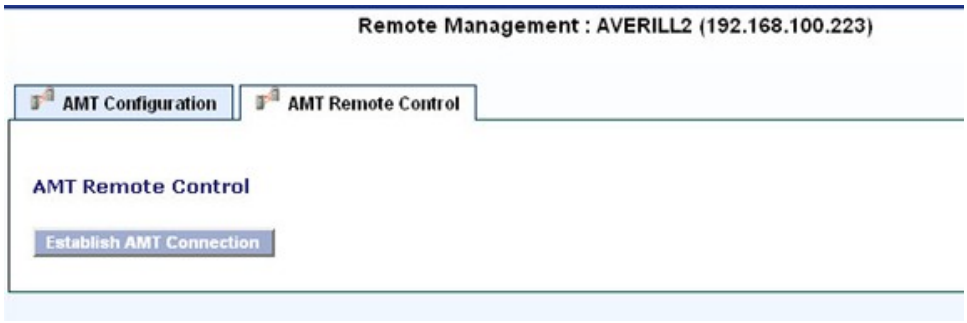


Figure 31: Establish AMT Connection

Once connected you can perform the following power options.

Power Off
This will perform a forced power off not a graceful shutdown.
Power On
This will perform a forced power on.
Power Reset
This will perform a power reset not a graceful reset.
Power Cycle Reset
This will perform a power cycle reset.

Serial Over LAN enables a user to remotely reboot a system. When a user reboots with SOL enabled, the SOL session is presented in the user's browser.

In order to create an SOL session, the user must verify the current power status.

Next, click the 'Launch SOL Session' box, and then click on the 'Send Command Button'.

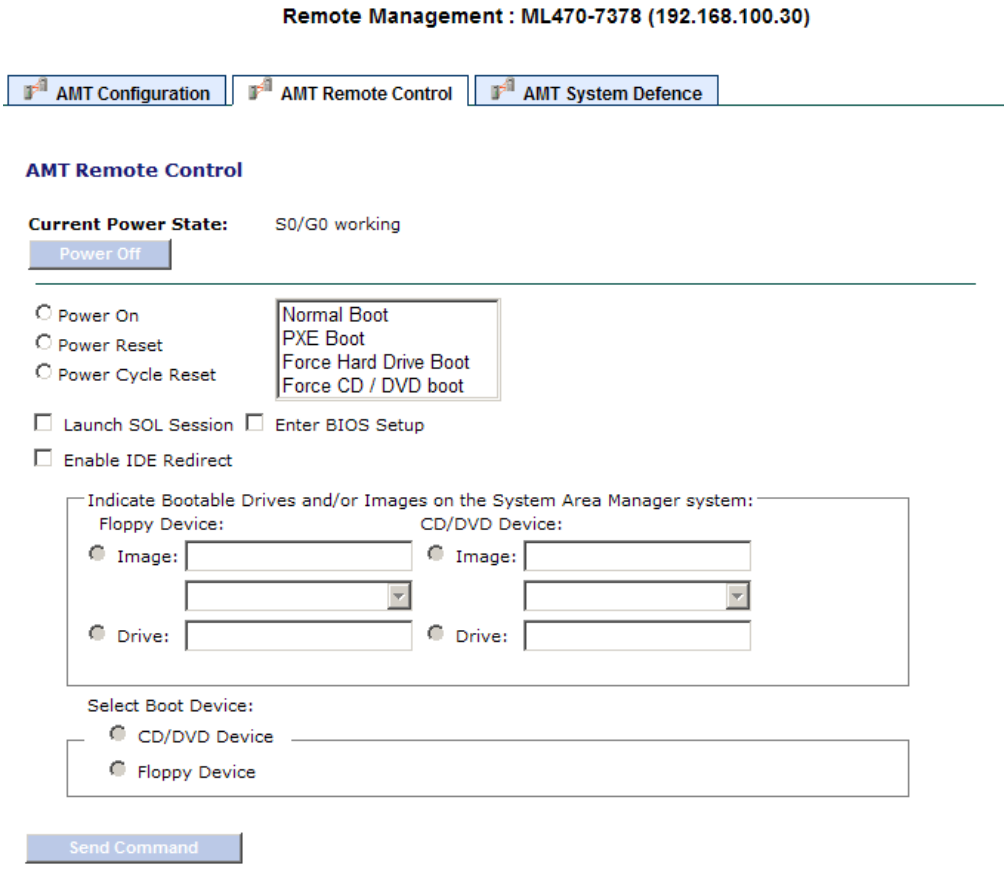


Figure 32: AMT Remote Control

Please Note: When using an SOL session, you are only able to boot the system normally. You cannot specify special commands such as PXE.

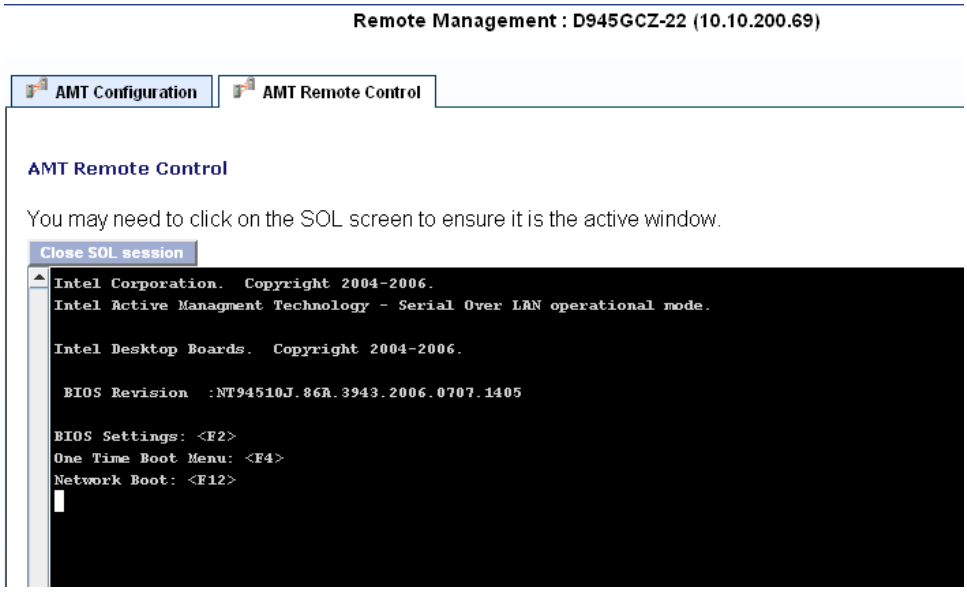

Remote Management : D945GCZ-22 (10.10.200.69)
AMT Configuration
AMT Remote Control
AMT Remote Control
You may need to click on the SOL screen to ensure it is the active window.
Close SOL session
Intel Corporation. Copyright 2004-2006.
Intel Active Managment Technology - Serial Over LAN operational mode.
Intel Desktop Boards. Copyright 2004-2006.
BIOS Revision :NT94510J.86A.3943.2006.0707.1405
BIOS Settings: <F2>
One Time Boot Menu: <F4>
Network Boot: <F12>

Figure 33: Serial Over LAN (In Use showing BIOS Re-configuration)

IDE-Redirect allows an AMT managed system on the System Area Manager tree to boot from an image, floppy, CD or DVD device which is located in the system running System Area Manager. IDE-Redirect is only available when using SOL.
Part of the AMT IDE Redirect process is verifying a valid image or device. If you do not have a physical floppy device you must chose the image as the Floppy Device. Both a floppy drive or image, AND a CD/DVD drive or image, must be specified. These drives or images are on the computer running System Area Manager, NOT on the computer running your web browser.

To invoke the IDE Redirect either click on the Power Reset or Power On buttons and click in the SOL and IDE-R check boxes. Under image or drive, indicate which image or drive you want the system to boot from, then select the boot device, and click 'Send Command'.

Figure 34: IDE-R (Configured to boot off CD-Rom)

When using either a Windows or Linux System Area Manager you need to use the correct corresponding Windows or Linux syntax for the Floppy disk device and CD ROM device.

If you are unsure of what the logical letter of the CD ROM device is, browse to the Storage screen of the System Area Manager.

If no floppy disk drive is present then you must select the bootable image.

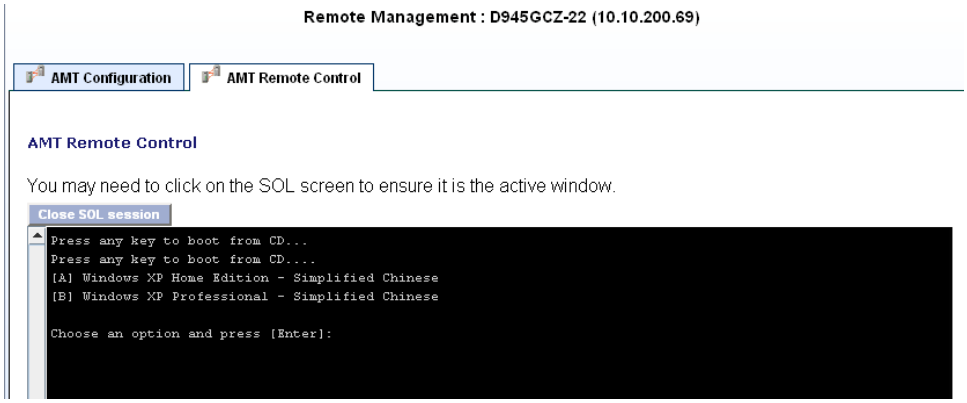

Remote Management : D945GCZ-22 (10.10.200.69)
AMT Configuration
AMT Remote Control
AMT Remote Control
You may need to click on the SOL screen to ensure it is the active window.
Close SOL session
Press any key to boot from CD...
Press any key to boot from CD....
[A] Windows XP Home Edition - Simplified Chinese
[B] Windows XP Professional - Simplified Chinese
Choose an option and press [Enter]:

Figure 35: IDE-R (In Use showing remote boot off CD-Rom)

Examples of IDE-R Drive and Image Syntax

System Area Manager running on a Windows Operating System

Floppy Device Drive **a:**
Floppy Device Image **c:\win98dos.img** or **c:\win98doscd.iso**

CD Rom Device Drive **d:**
CD Rom Device Image **c:\win98doscd.iso**

System Area Manager running on a Linux Operating System

Floppy Device Drive **/dev/fd0**

CD Rom Device Drive **/dev/hda**

System Defense allows the System Area Manager to define and enforce network security policies.

After clicking on the AMT System Defense tab, you will need to establish a connection with the AMT machine by clicking on the Establish AMT Connection button.

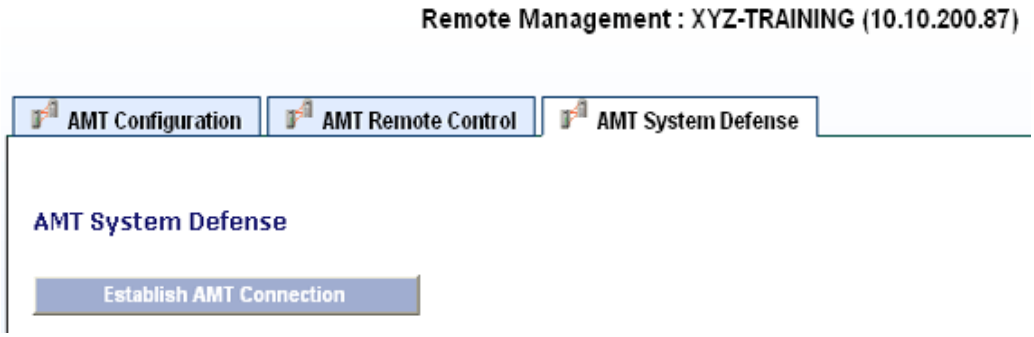


Figure 36: AMT System Defense (Establish AMT Connection)

When you first access the system defense screen, any policies that have been configured in the AMT Management Engine are presented.

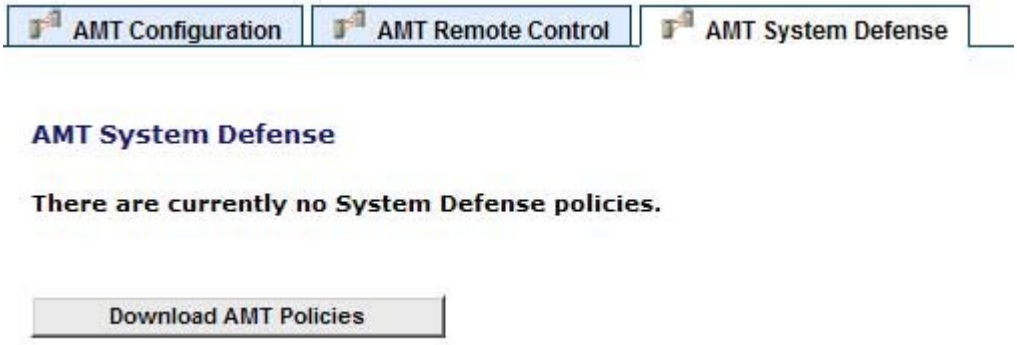


Figure 37: Download AMT Policies

If the AMT-Quarantine and the AMT-Management Policies are not programmed into the AMT Management Engine you will be presented with a download button. This will allow the AMT Policies to be configured in the AMT Management Engine.

The Screen will refresh automatically and then the two AMT-Management Policies policies will appear on the screen.

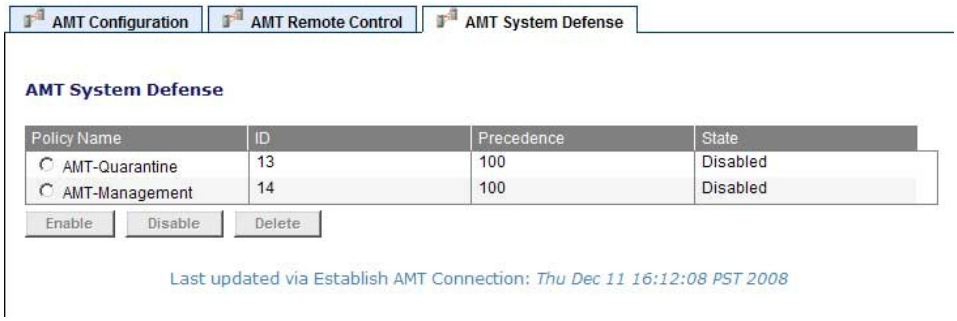


Figure 38: AMT System Defense Policies

Initially the three buttons enable, disable and delete are not available. Once you select a Policy, the Enable and Delete buttons become available. This allows you to enable a policy or remove the policy from the AMT Management Engine.

Once a policy is enabled, its status changes to active so you can see which policy is currently active. Only one policy may be enabled at a time.

When the currently active Policy is selected the Disable and Delete buttons become available. This allow the policy to be disabled or removed from the AMT Management Engine.

The “AMT-Quarantine” policy causes the Intel AMT device to block all packets to/from the operating system running on the client. So the administrator would have to go to the system to troubleshoot or repair the system.

The “AMT-Management” policy causes the Intel AMT device to block all packets to/from the operating system running on the client, except those sent to and from SyAM’s management components.

This allows the Administrator to access the Intel AMT client system using System Client remote console capability while the operating system is running, in order to inspect or repair the system, but without providing general access to/from the system.

IPMI Event Log

Server System Client can monitor physical events occurring on IPMI-enabled servers that are being managed. These events are recorded in the IPMI Event Log, which is accessible through System Area Manager. Each event is given a unique number and dated. This information, as well as a description of the event type, sensor type affected, and event alert type are recorded in the IPMI Event Log.

In addition, the IPMI event log lists the version of the log, the number of entries in the log, the last time an entry was added, the last time the log was cleared, and the free space remaining for the log.

The log can be reviewed/filtered by listing all events, or by filtering by an event range. The results can be displayed on the screen or exported to a file in a .CSV format without clearing the log.

The IPMI Event Log allows administrators to retrieve and view all events occurring and reported by a specific server. In order to access the IPMI Event Log, the system must be IPMI-enabled and running a valid version of Server System Client.

Fields included in this screen are:

- IPMI Version
- Number of entries in the log
- Last time an entry was made in the log
- Time of last log clear
- Free space

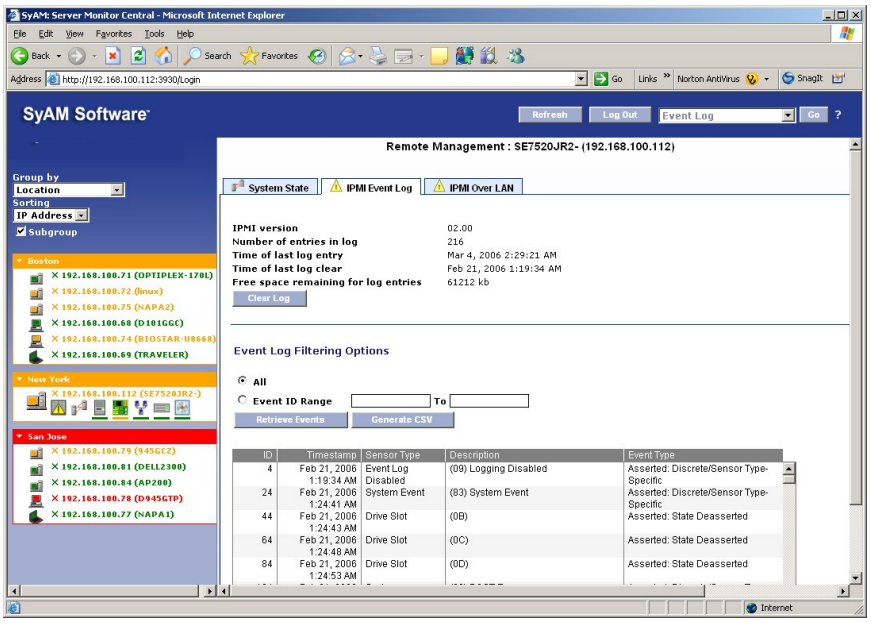


Figure 39: IPMI Event Log

The IPMI Event Log provides administrators with the option to clear or purge the log, by clicking the <clear> button. Note: this action cannot be undone.

IPMI Event Retrieval

The IPMI Event Log provides administrators with the option of retrieving and viewing some or all events recorded for the server, and sorting them by type.

To retrieve all of the events from the IPMI event log stored on the BMC, click on the radio button next to "All".

To retrieve a subset of events, enter a beginning and ending Event ID. The beginning Event ID value must be either 0 (to retrieve from the beginning of the log), or an actual Event ID number. You will receive an error message if a non-0 Event ID cannot be found.

Then click on the Retrieve button. he results will be displayed in the detail window at the bottom of the screen.

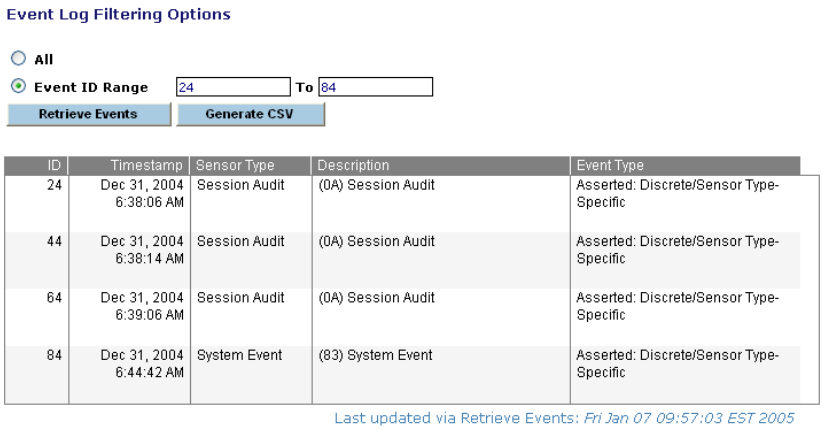


Figure 40: IPMI Event Log Retrieval

The ID values assigned to events are generated by the IPMI controller, and are dependent on how the system's firmware has been configured. As a result, the Event ID may differ by server platform.

Generate CSV
This button retrieves the events and saves them to a CSV file.

IPMI Over LAN

Server System Client can provide IPMI Over LAN power management and event log capabilities when the system is in either a operating system-present or -absent state.

You must first configure the BMC's IP address and Password using the vendor provided utilities before you can utilize this IPMI Over LAN feature.

Enter the user name, password and IP address of the BMC for the managed system, then click on the apply button to save this data.

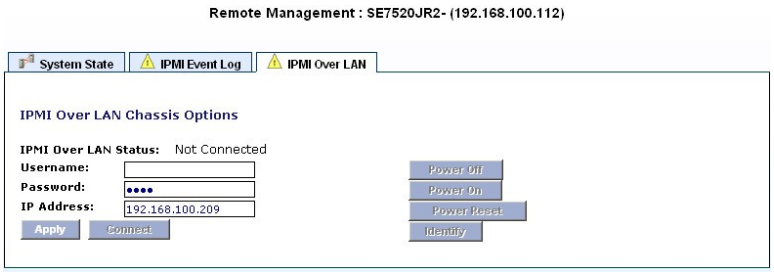


Figure 41: IPMI Over LAN – Enter details for accessing the BMC

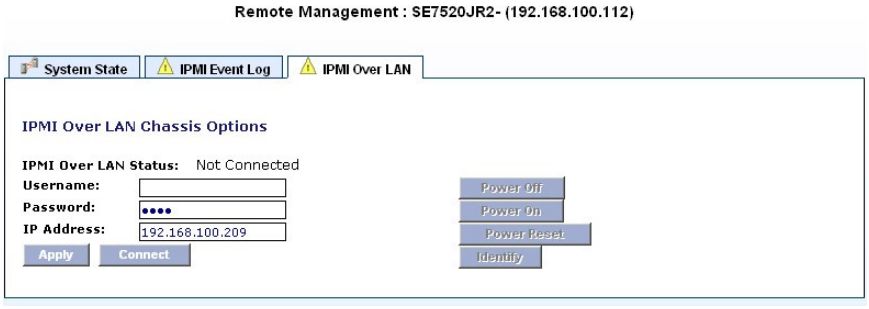


Figure 42: IPMI Over LAN – Details applied

Once you have saved the User name, password and IP Address you can click on the Connect button to access the managed system's BMC over the LAN.

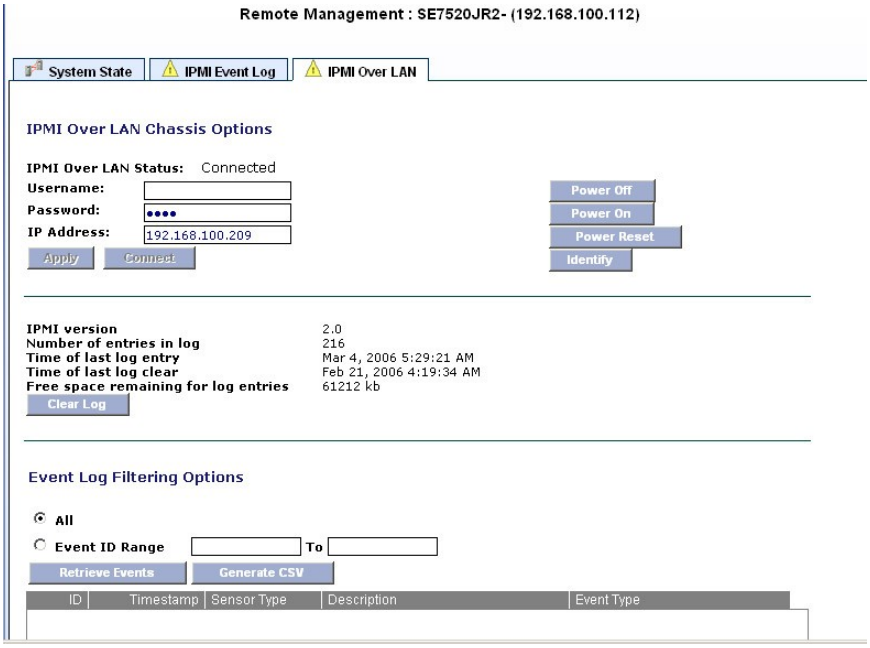


Figure 43: IPMI Over LAN – Connected

Once connected you can perform the following options.

Power Off

This will perform a forced power off not a graceful shutdown. T**he operating system may or may not receive notification and shut down, this varies by hardware platform.**

Power On

This will perform a forced power on.

Power Reset

This will perform a power reset not a graceful reset. **The operating system may or may not receive notification and shut down, this varies by hardware platform.**

Identify

This will light the identification LED of the system. This feature is not supported in all hardware platforms.

Event Log

The IPMI Event Log is accessed in exactly the same manner described above.

Chapter 6: Central Event Logging

This chapter provides instruction on how to access the System Area Manager Software's centralized event logging facility.

Administrators can use the SyAM event log to quickly identify trends across system events.

Central Event Logging

All systems being managed by System Area Manager (are present in the Management Tree) have their events automatically recorded in the System Area Manager Event Log.

Each event is dated, and lists the location of the event by system name, IP address, and category (storage, network, hardware, etc.)

Event Filtering

Below the Event Log screen is where you set the information to filter the event log by.

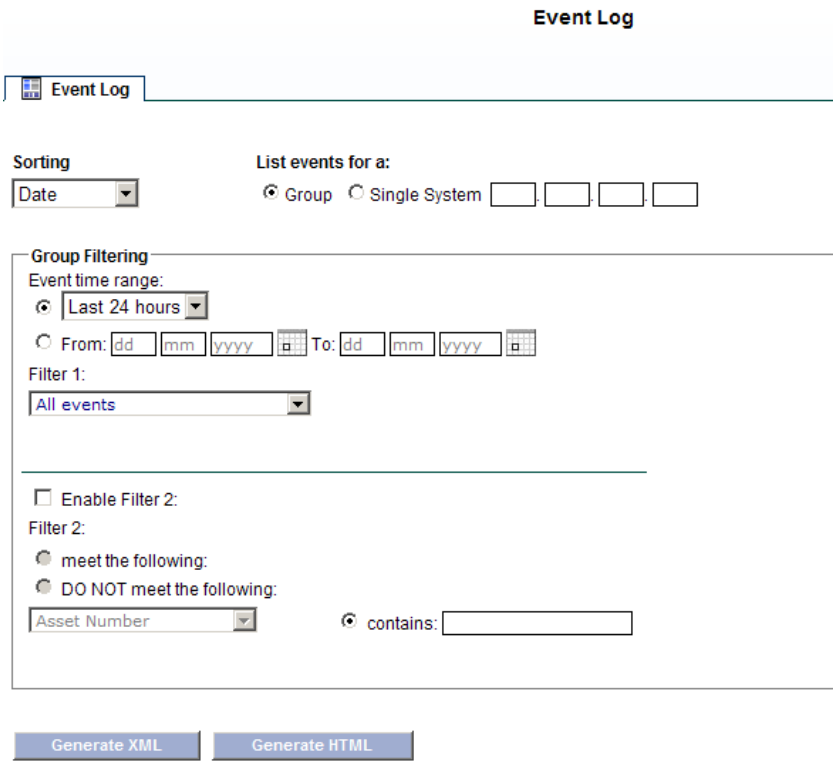


Figure 44: Event Log Filtering Options

Choose the Sorting

- Date
- Event Type
- Host Name
- IP Address

Group or Single System IP Address

Time Range

- Last 24 Hours
- Last 7 Days
- Last 30 days
- All
- Or choose a Date Range (From – To)

Next you can choose from Filter 1

- All Events
- Asset Monitoring Events
- Hardware Events
- Logical Disk Utilization Events
- Network Events
- Operator Events
- Performance Utilization Events
- Platform event Traps
- Storage Events
- System Absent Events

You can then set a second filter by clicking the Enable Filter 2 Check box

This filter can be set to meet the following criteria or DO NOT meet the Criteria.

- Asset Number
- Board Model
- Function
- Health
- Installed Applications
- Location
- Logical Free Disk Space
- Machine Model
- Operating System
- Owner
- Physical Disks

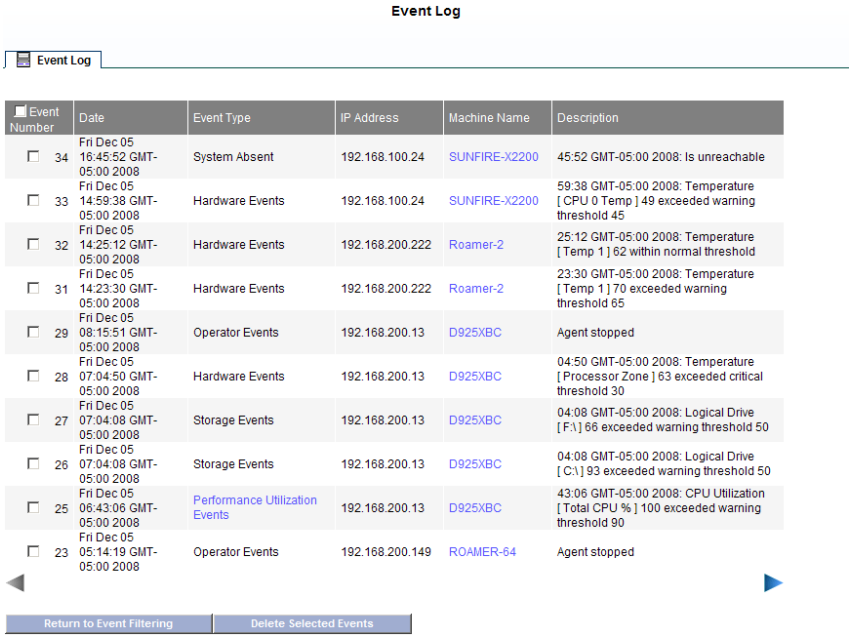
Once you have set you filter options you can either generate the results to screen by pressing the Generate HTML button or export them to XML by pressing the Generate XML button.

Viewing Events

Once you press the Generate HTML button a new page is opened showing the events within your filtered criteria.

10 Events are shown per page and you can go to the Next page or Back a page by pressing the arrows at the bottom of the page.

If a Performance Utilization Event has occurred you can click on the event type to open up the processes snap shot. This will be in Memory order for a Physical or Virtual Memory Utilization event or CPU order for a CPU Utilization event.



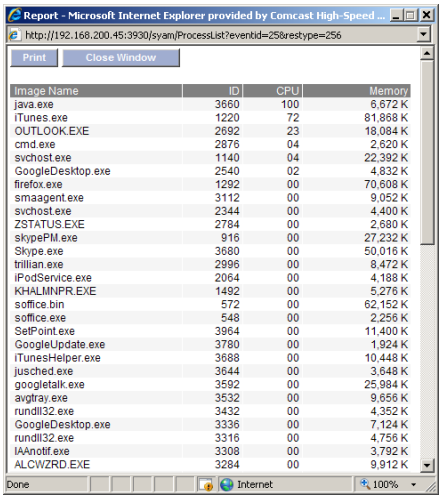
Event Log

Event Log

Event Number	Date	Event Type	IP Address	Machine Name	Description
34	Fri Dec 05 16:45:52 GMT-05:00 2008	System Absent	192.168.100.24	SUNFIRE-X2200	45:52 GMT-05:00 2008: Is unreachable
33	Fri Dec 05 14:59:38 GMT-05:00 2008	Hardware Events	192.168.100.24	SUNFIRE-X2200	59:38 GMT-05:00 2008: Temperature [CPU 0 Temp] 49 exceeded warning threshold 45
32	Fri Dec 05 14:25:12 GMT-05:00 2008	Hardware Events	192.168.200.222	Roamer-2	25:12 GMT-05:00 2008: Temperature [Temp 1] 62 within normal threshold
31	Fri Dec 05 14:23:30 GMT-05:00 2008	Hardware Events	192.168.200.222	Roamer-2	23:30 GMT-05:00 2008: Temperature [Temp 1] 70 exceeded warning threshold 65
29	Fri Dec 05 08:15:51 GMT-05:00 2008	Operator Events	192.168.200.13	D925XBC	Agent stopped
28	Fri Dec 05 07:04:50 GMT-05:00 2008	Hardware Events	192.168.200.13	D925XBC	04:50 GMT-05:00 2008: Temperature [Processor Zone] 63 exceeded critical threshold 30
27	Fri Dec 05 07:04:08 GMT-05:00 2008	Storage Events	192.168.200.13	D925XBC	04:08 GMT-05:00 2008: Logical Drive [F:\ ] 66 exceeded warning threshold 50
26	Fri Dec 05 07:04:08 GMT-05:00 2008	Storage Events	192.168.200.13	D925XBC	04:08 GMT-05:00 2008: Logical Drive [C:\ ] 93 exceeded warning threshold 50
25	Fri Dec 05 06:43:06 GMT-05:00 2008	Performance Utilization Events	192.168.200.13	D925XBC	43:06 GMT-05:00 2008: CPU Utilization [Total CPU %] 100 exceeded warning threshold 90
23	Fri Dec 05 05:14:19 GMT-05:00 2008	Operator Events	192.168.200.149	ROAMER-64	Agent stopped

Return to Event Filtering | Delete Selected Events

Figure 45: Viewing the HTML Event Log on screen



Report - Microsoft Internet Explorer provided by Comcast High-Speed ...

http://192.168.200.45:3930/syam/ProcessList?eventid=25&restype=256

Print | Close Window

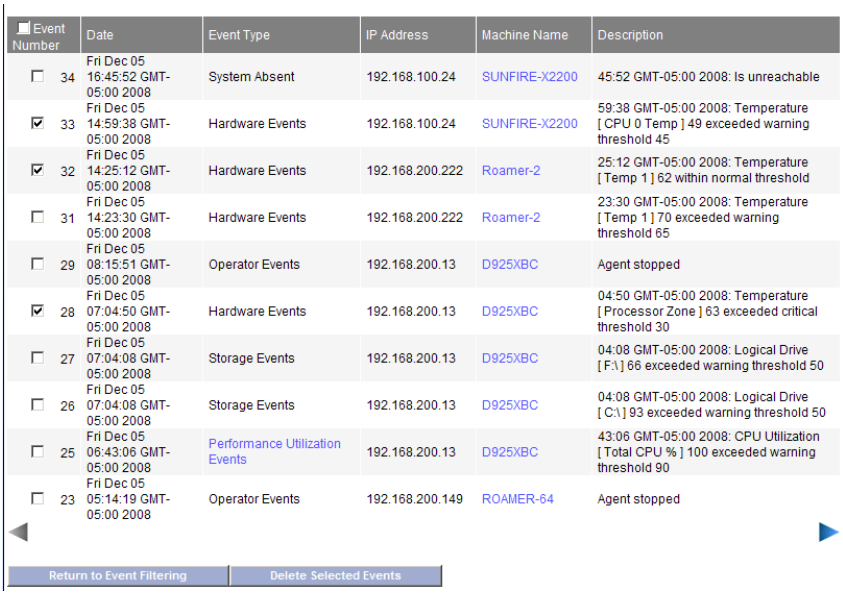
Image Name	ID	CPU	Memory
java.exe	3660	100	6,672 K
iTunes.exe	1220	72	81,868 K
OUTLOOK.EXE	2692	23	18,084 K
cmd.exe	2876	04	2,620 K
svchost.exe	1140	04	22,392 K
GoogleDesktop.exe	2540	02	4,832 K
firefox.exe	1292	00	70,608 K
smaagent.exe	3112	00	9,052 K
svchost.exe	2344	00	4,400 K
ZSTATUS.EXE	2784	00	2,680 K
skypePM.exe	916	00	27,232 K
Skype.exe	3680	00	50,016 K
trillian.exe	2996	00	8,472 K
iPodService.exe	2064	00	4,188 K
KHALMNPR.EXE	1492	00	5,276 K
soffice.bin	572	00	62,152 K
soffice.exe	548	00	2,256 K
SetPoint.exe	3964	00	11,400 K
GoogleUpdate.exe	3780	00	1,924 K
iTunesHelper.exe	3688	00	10,448 K
jusched.exe	3644	00	3,648 K
googletalk.exe	3592	00	25,984 K
avgtray.exe	3532	00	9,656 K
rundll32.exe	3432	00	4,352 K
GoogleDesktop.exe	3336	00	7,124 K
rundll32.exe	3316	00	4,756 K
IAAnotif.exe	3308	00	3,792 K
ALCWZRD.EXE	3284	00	9,912 K

Done | Internet | 100%

Figure 46: Viewing the Process Snap Shot for a Memory Utilization Event

Deleting Events from the Event Log

You can remove events from the event log by clicking on their check box and pressing the Deleted Selected Events button. You can choose all events on the page by clicking on the check box in the header bar next to Event Number.



Event Number	Date	Event Type	IP Address	Machine Name	Description
☐ 34	Fri Dec 05 16:45:52 GMT-05:00 2008	System Absent	192.168.100.24	SUNFIRE-X2200	45:52 GMT-05:00 2008: Is unreachable
☑ 33	Fri Dec 05 14:59:38 GMT-05:00 2008	Hardware Events	192.168.100.24	SUNFIRE-X2200	59:38 GMT-05:00 2008: Temperature [CPU 0 Temp] 49 exceeded warning threshold 45
☑ 32	Fri Dec 05 14:25:12 GMT-05:00 2008	Hardware Events	192.168.200.222	Roamer-2	25:12 GMT-05:00 2008: Temperature [Temp 1] 62 within normal threshold
☐ 31	Fri Dec 05 14:23:30 GMT-05:00 2008	Hardware Events	192.168.200.222	Roamer-2	23:30 GMT-05:00 2008: Temperature [Temp 1] 70 exceeded warning threshold 65
☐ 29	Fri Dec 05 08:15:51 GMT-05:00 2008	Operator Events	192.168.200.13	D925XBC	Agent stopped
☑ 28	Fri Dec 05 07:04:50 GMT-05:00 2008	Hardware Events	192.168.200.13	D925XBC	04:50 GMT-05:00 2008: Temperature [Processor Zone] 63 exceeded critical threshold 30
☐ 27	Fri Dec 05 07:04:08 GMT-05:00 2008	Storage Events	192.168.200.13	D925XBC	04:08 GMT-05:00 2008: Logical Drive [F:\ ] 66 exceeded warning threshold 50
☐ 26	Fri Dec 05 07:04:08 GMT-05:00 2008	Storage Events	192.168.200.13	D925XBC	04:08 GMT-05:00 2008: Logical Drive [C:\ ] 93 exceeded warning threshold 50
☐ 25	Fri Dec 05 06:43:06 GMT-05:00 2008	Performance Utilization Events	192.168.200.13	D925XBC	43:06 GMT-05:00 2008: CPU Utilization [Total CPU %] 100 exceeded warning threshold 90
☐ 23	Fri Dec 05 05:14:19 GMT-05:00 2008	Operator Events	192.168.200.149	ROAMER-64	Agent stopped

Figure 47: Deleting Events

Chapter 7: Central Reporting

This chapter provides instruction on how to access the reporting capabilities within the System Area Manager Software.

Administrators can quickly and efficiently produce summary or detailed reports on their Server, Desktop and Notebook assets.

Reporting

Through the System Area Manager software, administrators can run a variety of reports on the managed systems that it monitors, view it on screen, and print or export to file in CSV or XML format. You can choose to report on a single managed system, a group of systems, or using filters a user defined set of managed systems.

Administrators are given the option of sorting the report by Machine name or IP address.

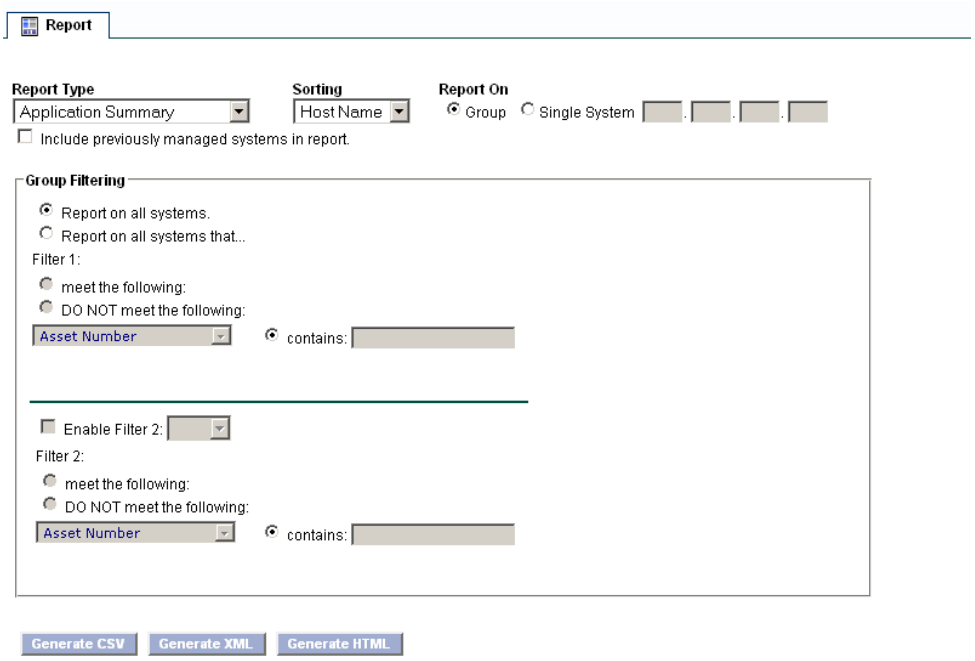


Figure 48: System Area Manager Reports

Report Type

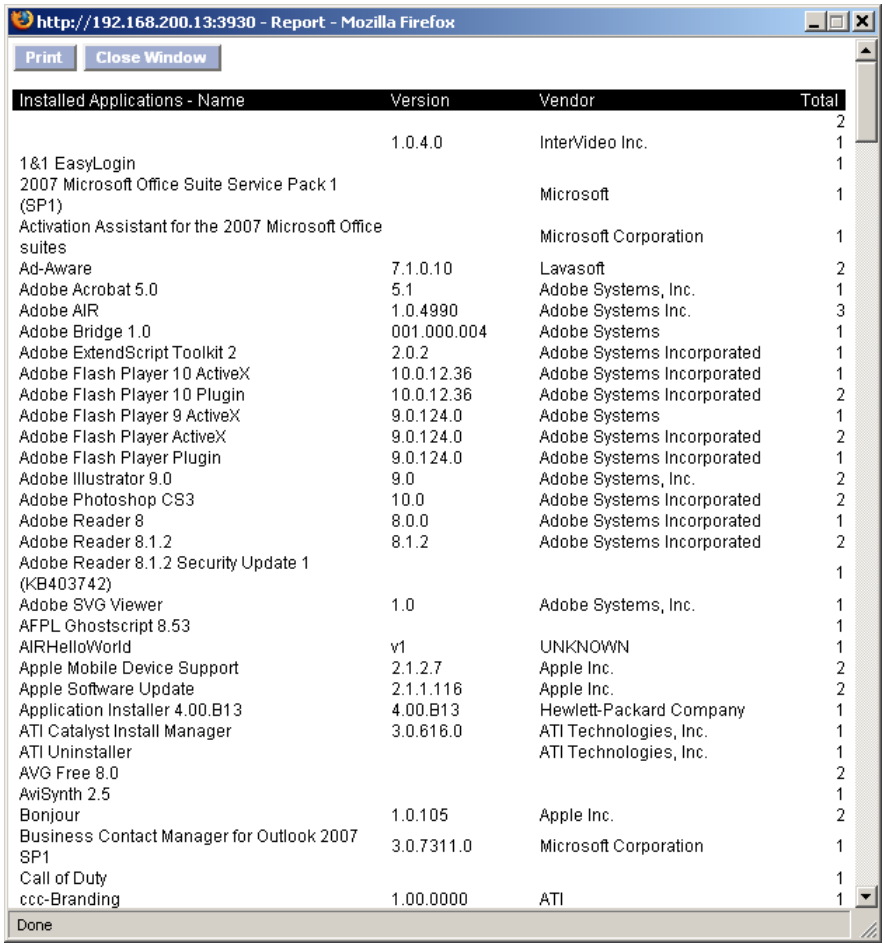
There are 6 different report types to choose from

- Application Summary
- Asset Details
- Asset List
- Asset Summary
- Operating System Summary
- Power Audit

Application Summary Report

The Application summary report will contain the following information:

- Application Name
- Version
- Vendor
- Total Quantitiy installed



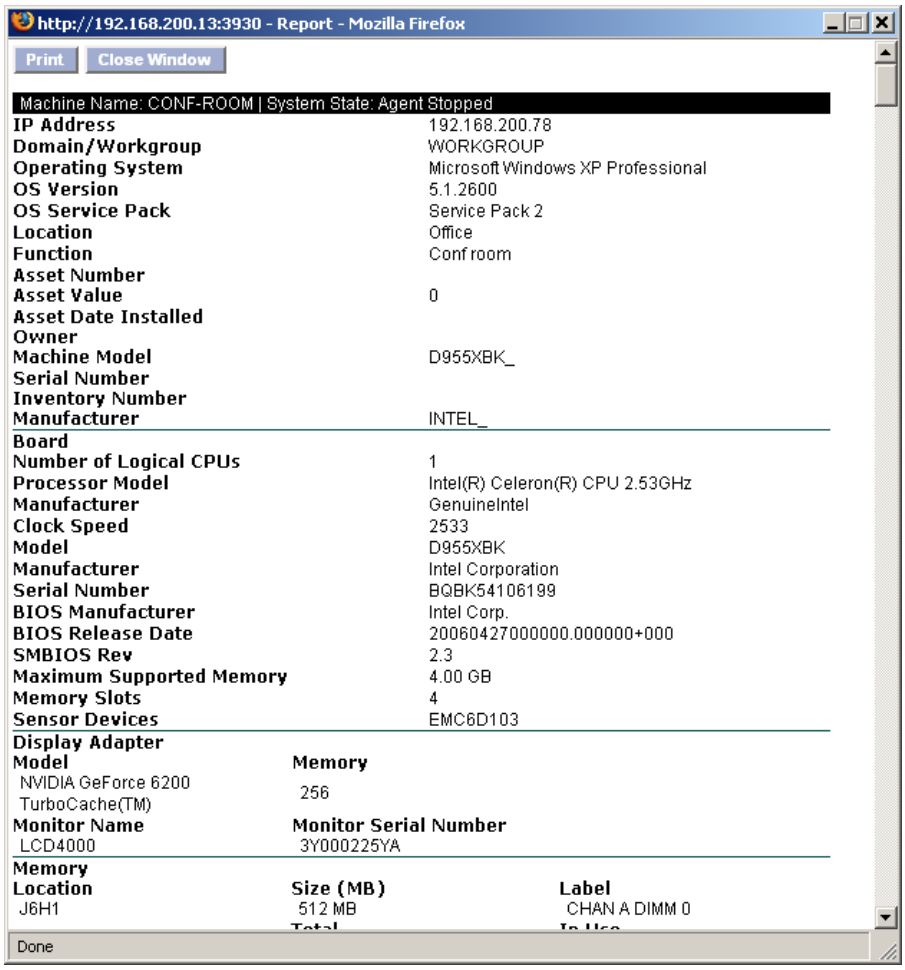
Installed Applications - Name	Version	Vendor	Total
			2
	1.0.4.0	InterVideo Inc.	1
1&1 EasyLogin			1
2007 Microsoft Office Suite Service Pack 1 (SP1)		Microsoft	1
Activation Assistant for the 2007 Microsoft Office suites		Microsoft Corporation	1
Ad-Aware	7.1.0.10	Lavasoft	2
Adobe Acrobat 5.0	5.1	Adobe Systems, Inc.	1
Adobe AIR	1.0.4990	Adobe Systems Inc.	3
Adobe Bridge 1.0	001.000.004	Adobe Systems	1
Adobe ExtendScript Toolkit 2	2.0.2	Adobe Systems Incorporated	1
Adobe Flash Player 10 ActiveX	10.0.12.36	Adobe Systems Incorporated	1
Adobe Flash Player 10 Plugin	10.0.12.36	Adobe Systems Incorporated	2
Adobe Flash Player 9 ActiveX	9.0.124.0	Adobe Systems	1
Adobe Flash Player ActiveX	9.0.124.0	Adobe Systems Incorporated	2
Adobe Flash Player Plugin	9.0.124.0	Adobe Systems Incorporated	1
Adobe Illustrator 9.0	9.0	Adobe Systems, Inc.	2
Adobe Photoshop CS3	10.0	Adobe Systems Incorporated	2
Adobe Reader 8	8.0.0	Adobe Systems Incorporated	1
Adobe Reader 8.1.2	8.1.2	Adobe Systems Incorporated	2
Adobe Reader 8.1.2 Security Update 1 (KB403742)			1
Adobe SVG Viewer	1.0	Adobe Systems, Inc.	1
AFPL Ghostscript 8.53			1
AIRHelloWorld	v1	UNKNOWN	1
Apple Mobile Device Support	2.1.2.7	Apple Inc.	2
Apple Software Update	2.1.1.116	Apple Inc.	2
Application Installer 4.00.B13	4.00.B13	Hewlett-Packard Company	1
ATI Catalyst Install Manager	3.0.616.0	ATI Technologies, Inc.	1
ATI Uninstaller		ATI Technologies, Inc.	1
AVG Free 8.0			2
AviSynth 2.5			1
Bonjour	1.0.105	Apple Inc.	2
Business Contact Manager for Outlook 2007 SP1	3.0.7311.0	Microsoft Corporation	1
Call of Duty			1
ccc-Branding	1.00.0000	ATI	1

Figure 49: Application Summary Report

Asset Detailed Report

The Asset detailed report will contain the following additional information:

-
-
- Machine Name
- Health State
- IP Address
- Operating System Version / Service Pack
- Location
- Function
- Asset Number / Value / Date Installed / Owner
- Machine Model / Serial Number / Inventory Number / Manufacturer
- Number of Logical CPU's and type
- Total amount of Physical and Virtual Memory installed and number of Memory banks used
- Number of Logical Disks and capacity available
- RAID Controllers installed
- Number of Installed Applications
- Board Model / Manufacturer
- Sensor Devices Discovered
- Display Adapter Model/Memory
- Monitor Name / Serial Number
- Total amount of Memory installed
- Individual Memory Bank Label and Capacity
- Virtual and Physical Total Memory and Memory in Use
- Total Physical Disk capacity
- Physical disk Size / Device Information
- Individual Physical disk Label and Capacity
- Logical drive – Letter – Available and Total Capacity
- RAID Controller Model / Status / RAID Level / Capacity / # Drives
- Removable Device Name / Description
- Network Adapter Number / Description / DHCP / IP Address / MAC Address
- PCI Slot Label and Status
- Applications Installed – Name / Vendor / Version


http://192.168.200.13:3930 - Report - Mozilla Firefox
Print
Close Window
Machine Name: CONF-ROOM | System State: Agent Stopped
IP Address 192.168.200.78
Domain/Workgroup WORKGROUP
Operating System Microsoft Windows XP Professional
OS Version 5.1.2600
OS Service Pack Service Pack 2
Location Office
Function Conf room
Asset Number
Asset Value 0
Asset Date Installed
Owner
Machine Model D955XBK_
Serial Number
Inventory Number
Manufacturer INTEL_
Board
Number of Logical CPUs 1
Processor Model Intel(R) Celeron(R) CPU 2.53GHz
Manufacturer GenuineIntel
Clock Speed 2533
Model D955XBK
Manufacturer Intel Corporation
Serial Number BQBK54106199
BIOS Manufacturer Intel Corp.
BIOS Release Date 20060427000000.000000+000
SMBIOS Rev 2.3
Maximum Supported Memory 4.00 GB
Memory Slots 4
Sensor Devices EMC6D103
Display Adapter
Model
NVIDIA GeForce 6200 TurboCache(TM)
Memory
256
Monitor Name
LCD4000
Monitor Serial Number
3Y000225YA
Memory
Location
J6H1
Size (MB)
512 MB
Label
CHAN A DIMM 0
Done

Asset List Report

The Asset list report will contain the following information:

- Machine Name
- IP Address
- Operating System
- Location

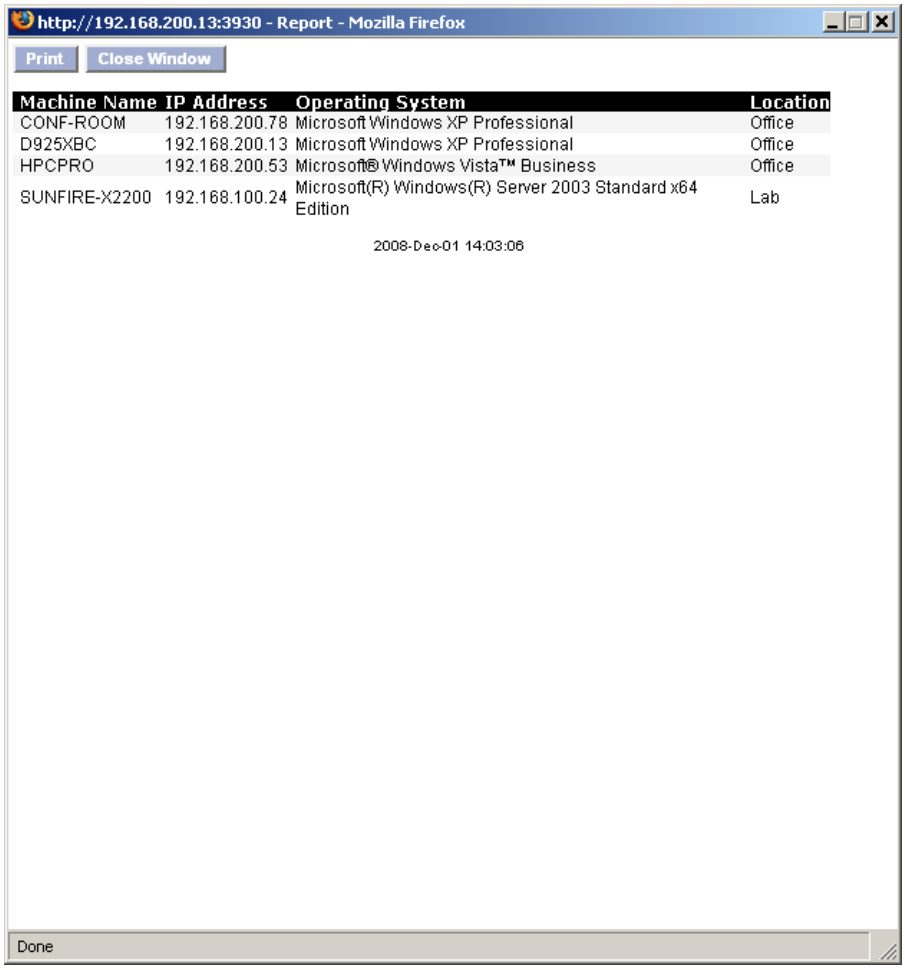

http://192.168.200.13:3930 - Report - Mozilla Firefox
Print
Close Window
Machine Name IP Address Operating System Location
CONF-ROOM 192.168.200.78 Microsoft Windows XP Professional Office
D925XBC 192.168.200.13 Microsoft Windows XP Professional Office
HPCPRO 192.168.200.53 Microsoft® Windows Vista™ Business Office
SUNFIRE-X2200 192.168.100.24 Microsoft(R) Windows(R) Server 2003 Standard x64 Edition Lab
2008-Dec-01 14:03:06
Done

Figure 50: Asset List Report

Asset Summary Report

The Asset summary report will contain the following information:

- Machine Name
- Health State
- IP Address
- Operating System Version / Service Pack
- Location
- Function
- Asset Number / Value / Date Installed / Owner
- Machine Model / Serial Number / Inventory Number / Manufacturer
- Number of Logical CPU's and type
- Total amount of Physical and Virtual Memory installed and number of Memory banks used
- Number of Logical Disks and capacity available
- RAID Controllers installed
- Number of Installed Applications

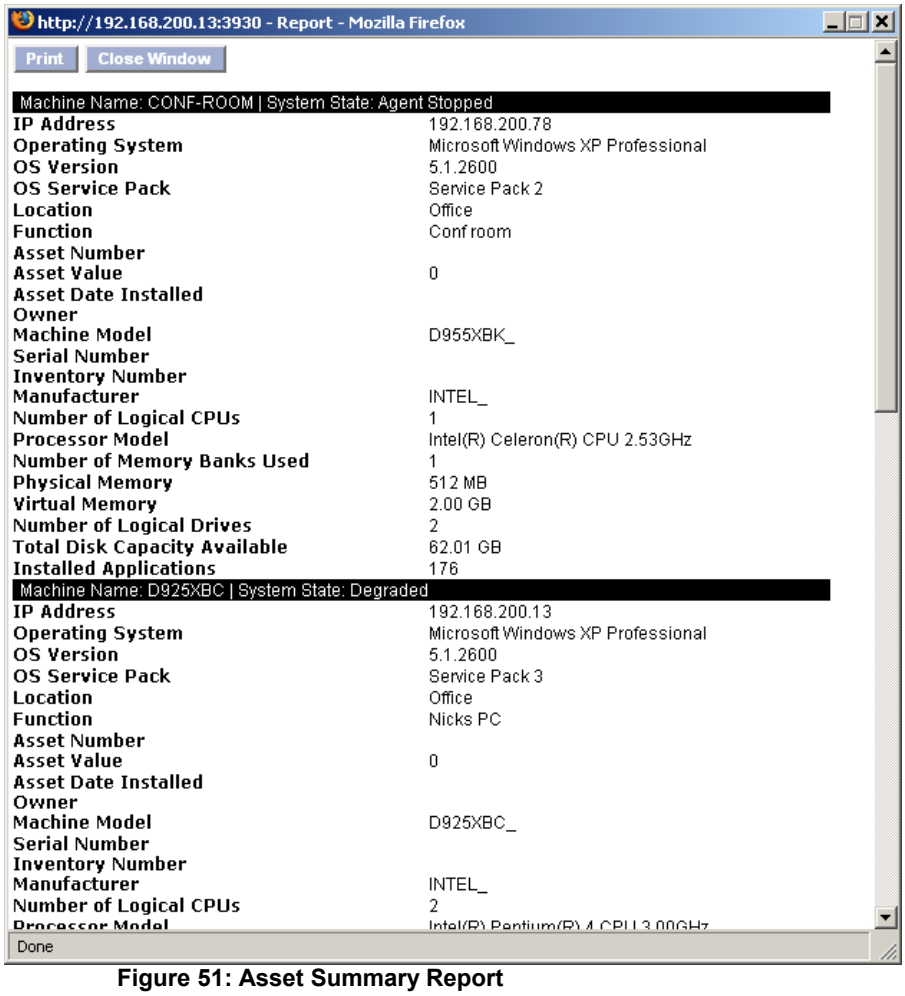


Figure 51: Asset Summary Report

Operating System Summary Report

The Operating System summary report will contain the following information:

- Operating System
- OS Version
- OS Service Pack
- Total Deployed

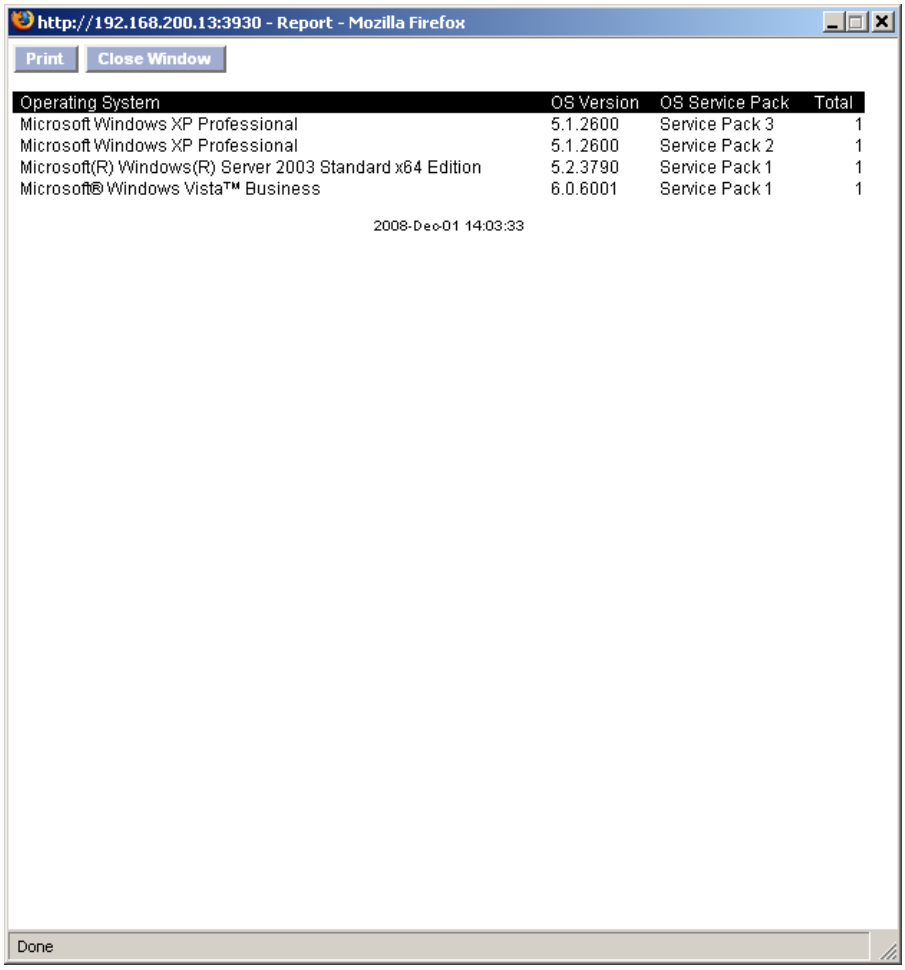


Figure 52: Operating System Summary Report

Power Audit Report

The Power Audit report will summerize the following information:

- Period for the report
- Total Hours in Period
- Number of Desktops and Number of Servers
- Total Hours On
- Total Hours Off
- Scheduled Off %
- Unscheduled Off %

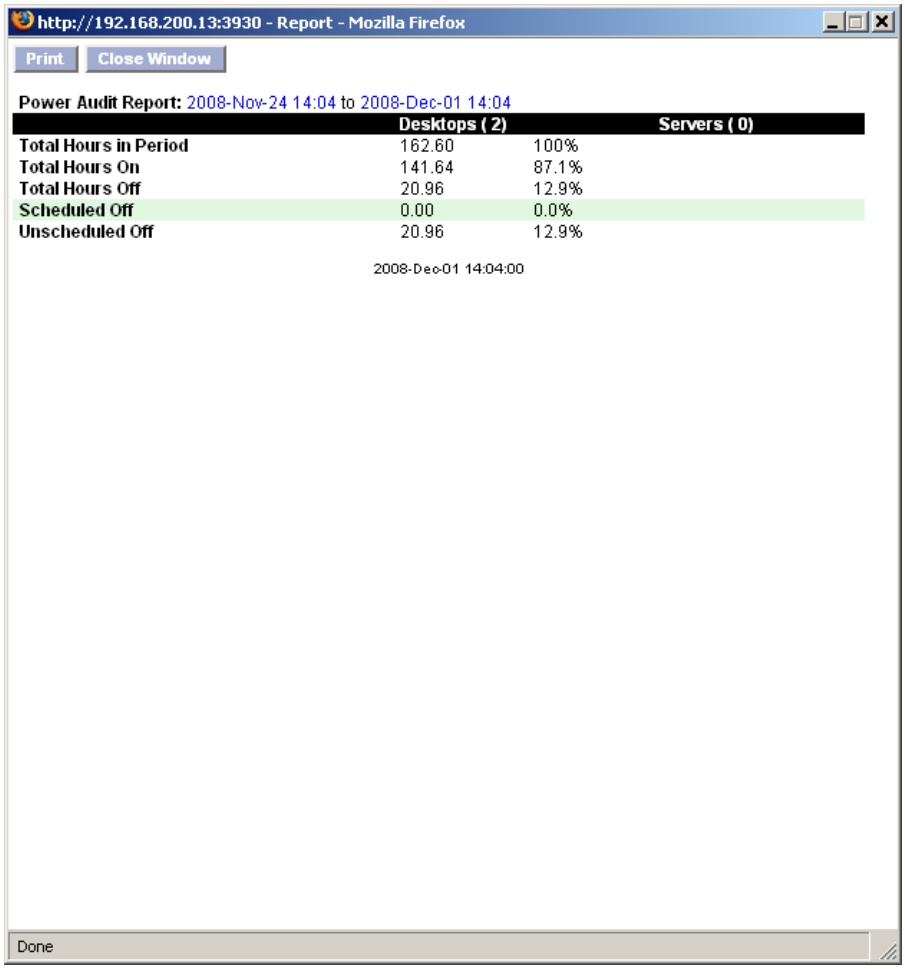


Figure 53: Power Audit Report

Chapter 8: Configuring System and Central Alerts

SyAM System Area Manager software provides the ability to configure alerts at individual system and central levels.

By using System Area Manager users may configure thresholds, and sample/reset periods for each monitored resource. And several new notification methods become available, such as via SNMP Traps or Operating System Event Logs.

System Alert Matrix – System Level Alerting

The System Alert Matrix provides a detailed, color-coded view of the status of all monitored components in a specific managed system.

Settings such as notification methods, thresholds, sample periods, etc for each sensor type category are automatically applied to all discovered sensor instances of that type.

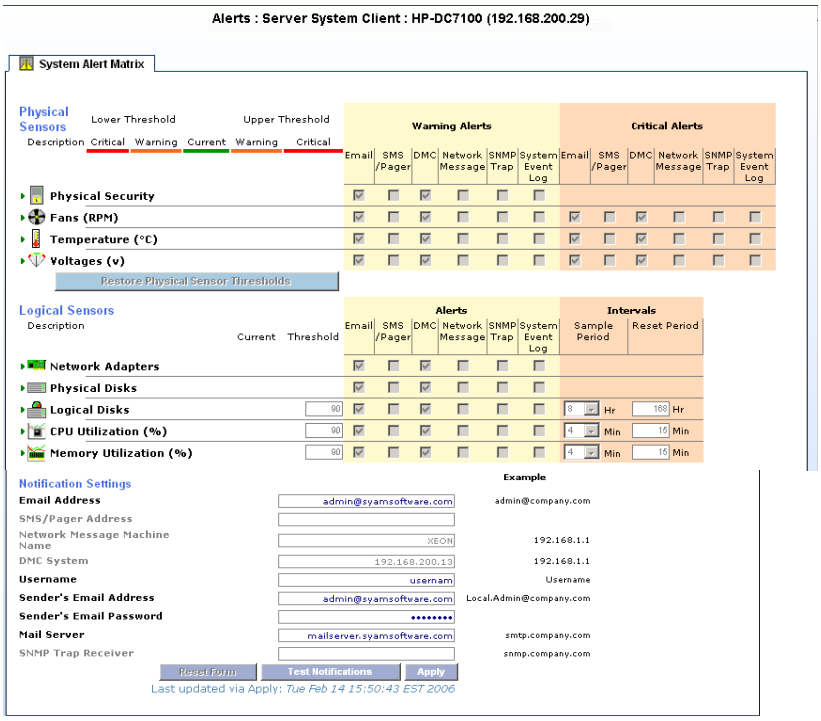


Figure 54: System Alert Matrix

Monitored Sensor Types

Physical Sensors

	Security – If/when the system chassis is opened, the intrusion will trigger a sensor alert, provided that the connected board/BIOS support this information reporting.
	Fans – Monitored for rotational speed provided the fan is connected to a board/BIOS that supports the information reporting.
	Voltages – Monitored for the functionality that the connected board/BIOS supports.
	Temperature – Monitored for the functionality that the connected board/BIOS supports.
	Thermal Controlled Fans – Monitored for rotational speed, alerts when the CPU Temperature exceeds the defined threshold and the fan is not spinning. Provided for a defined set of motherboards supporting this feature.
	Redundant Power Loss – Monitors IPMI managed servers and alerts upon when redundant power systems loose their redundancy

Logical Sensors

	Network Adapters – Monitors Ethernet operational state.
	Physical Disk – Monitors the presence and percent usage of a physical disk in the system and/or a RAID Set available to the operating system through a RAID controller.
	Logical Disks – The percent of capacity used by the logical disk formatted and mounted by the operating system is reported. If the disk has not been formatted, it will be reported as a failed disk. Removable Device – Removable devices that are represented to the operating system will be reported as mounted as long as they are present in the system.
	Managed RAID Controller – RAID Controller health.
	Total CPU utilization – Percentage of CPU usage.
	Total Memory utilization – Percentage of Physical and Virtual Memory usage.
	Memory Error Rate – Number of Single- and Multi- Bit errors that have occurred (requires ECC memory and support by the server board)

Notification Settings

When a system is managed from the System Area Manager, it enables users to modify any of the thresholds, sample periods, reset periods, and notification methods. It also enables alerts to be sent via the other notification methods such as SMS/pager, Network Message, send to the SyAM System Area Manager perform central alerting methods), SNMP Trap, or write the event to the System Event Log. (Note this System Event Log means events will be written to the local Windows Event Log or Linux syslog.) Clicking on each sensor category tree expands it to reveal all instances in the category. To select an entire category of sensors for the alert, click on the bolded category header. To select individual instances, click on the appropriate boxes for each instance.

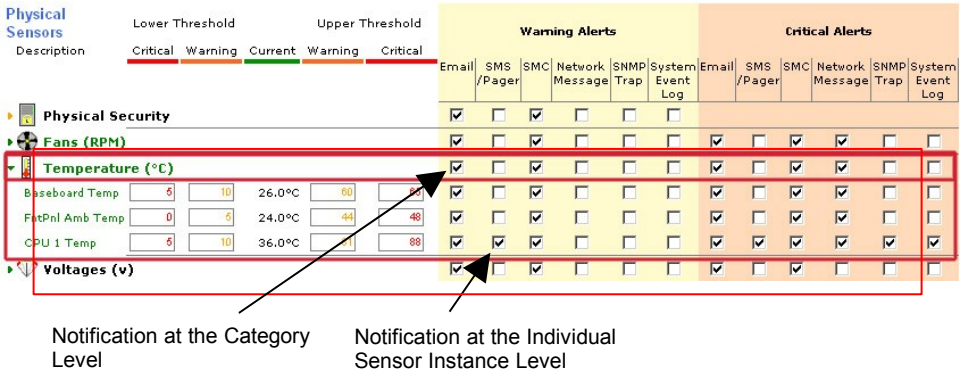


Figure 55: Setting Category and Instance-Level Notifications

Each sensor category provides the default notification options, thresholds, sample periods and reset periods that will automatically be applied to newly discovered sensor instances within that category.

Disabling Notifications

If you wish to disable notifications for a specific senor or sensor category you can by clicking on the No Monitoring check box.

This disables the sensor instance or sensor category from having any alerts notified, thus they will not be monitored or be represented in the health state of that sensor category, section the system or systems health.

Physical Sensor Upper and Lower Thresholds
Each physical sensor instance has its own range of safe operating values with lower and upper warning and critical thresholds. These values are discovered if the hardware platform supports that information, or are calculated from available data.

Physical Sensor Warning and Critical Alerts
Since physical sensors may enter warning or critical health states, separate alerting methods may be configured for each.

Logical Sensor Thresholds
Monitored resources that are not physical sensors are called "Logical Sensors". Each instance of the logical sensor types Logical Disk, CPU Utilization, and Memory Utilization, has a utilization threshold.

Logical Sensor Warning Alerts
Logical sensors, by design, may enter the warning health state but not critical. So there is only a single set of alerting methods available.

Sample Period
CPU and Memory Utilization are gathered several times over a period of time, so that transient spikes are not reported. This time period is configurable by the administrator, and is known as the sample period. The pre-set sample period options are from 4-8 minutes. If 80% of the gathered readings exceed the threshold, a transition to warning state occurs.

The sample period for an instance of Logical Disk that is a removable device (floppy or CD-ROM drive) is similar to that of other sensors. A set of four readings is gathered during the sample period. If the device (floppy disk or CD) is present through all of them, a transition to warning state occurs.

Reset Period
When a logical sensor transitions to a warning health state, an event is raised and alerts are sent according to the Warning Alerts settings. The reset period is the amount of time during which no additional alerts will be issued after the initial alert.

Removing a Sensor Instance From the System Alert Matrix
When a sensor instance, such as a specific logical or physical disk, has been removed from the system, or has otherwise entered a critical state, it is displayed in red and an "X" appears next to it. Click on the "X" to permanently delete this sensor instance from the alert matrix. Only do this if the instance is not being replaced. Once the sensor has been replaced it will automatically be monitored and the new health state will be represented.

Notification Settings – Configuring email alerting

Figure 56: Entering Notification Information

Enter the destination email address, the sender's email address, and the mail server hostname or IP address. Enter the user name and password if outgoing email is authenticated. Click the Apply button to save changes. Use the Test Notification button to send a test email, and ensure your configuration is correct.

Central Alert Matrix

The Central Alert Matrix is accessed from the Drop down menu on the header bar . It provides the ability to configure the appropriate notification options for events that are sent to this System Area Manager, from all of the systems it is managing.

Notifications can be configured to be sent via email, SMS/Pager and can be assigned to administrator one or two for each type of event, in addition to sending SNMP Traps.

Types of monitored events

	Platform Event Traps PET's – PET 1.0 formatted SNMP traps received are converted to plain text and alerted upon.
	Hardware Events – When a threshold is exceeded by a physical component within the system. Hardware Events include: physical chassis security, fan speed variation, chassis temperature fluctuation, voltage fluctuation or power redundancy loss
	Network Events – Network connectivity is lost due to an adapter failure.
	Storage Events – A logical disk has reached its utilization threshold, a logical or physical disk is lost (removed or not functioning), or a removable disk has remained present on the system for an extended period of time and may cause boot up issues.
	Performance Utilization Events – CPU or memory utilization threshold has been exceeded.
	Asset Monitoring Events – Server System Client records an inventory of the system components being monitored (i.e. CPUs, Memory, Disks, Software applications installed or removed, etc), and compares it each time the system is booted. Any discrepancy in the information when the agent is started is reported as an asset-monitoring event.
	System Absent Events – When the System Area Manager is no longer able to communicate with a managed system, it is reported as being absent, unless it was correctly shutdown.

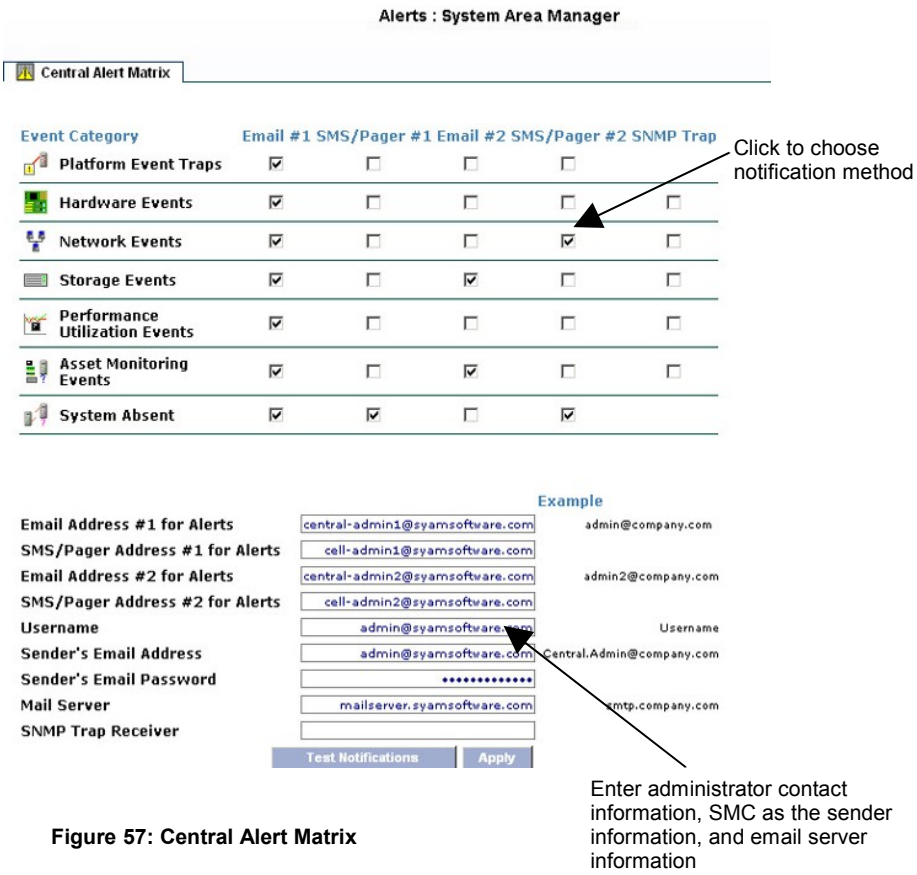


Figure 57: Central Alert Matrix

Integration into Enterprise Frameworks

System Area Management (SyAM) MIB

The SyAM MIB must be installed into the Enterprise Framework server before it can decipher traps sent from a managed system.

Please consult your Enterprise Framework application on how to install a 3rd party MIB.

The MIB file is installed in <Installed Directory>/system_monitor/syam.mib.

System Area Management (SyAM) Integration into Microsoft Operations Manager (MOM)

The SyAM Management Pack for Microsoft Operations Manager must be loaded into the MOM server, before it can decipher Windows events written by SyAM Management Agents. Also the MOM agent must be configured on each managed system to forward events to the MOM server.

Please consult your MOM documentation on how to load 3rd party Management Packs into the MOM server, and how to configure the MOM agent.

The MOM Management Pack file is installed in:
<InstalledDirectory>/system_monitor/syam.akm.

Chapter 9: Accessing System Information

This chapter provides instruction on how to access a managed system to obtain detailed information from each of the the sections/tabs.

System Detail Tab

The System Tab displays detailed information on the system's configuration, including BIOS, vendor information, operating system, location, machine name, function, memory and CPU utilization, etc. Administrators can choose to enter additional system information by filling in the fields at the top of the screen. The system's power management policies can be viewed and re-configured remotely by clicking on the Power Management button.

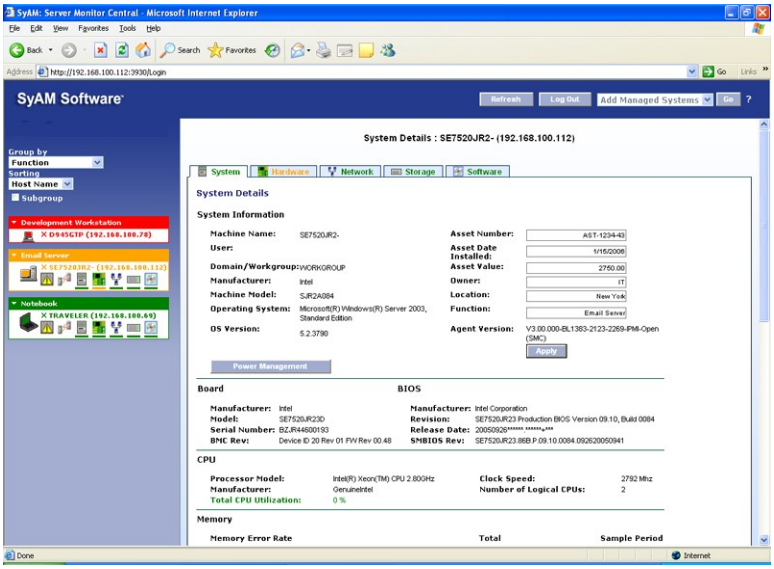


Figure 58: System Detail Tab

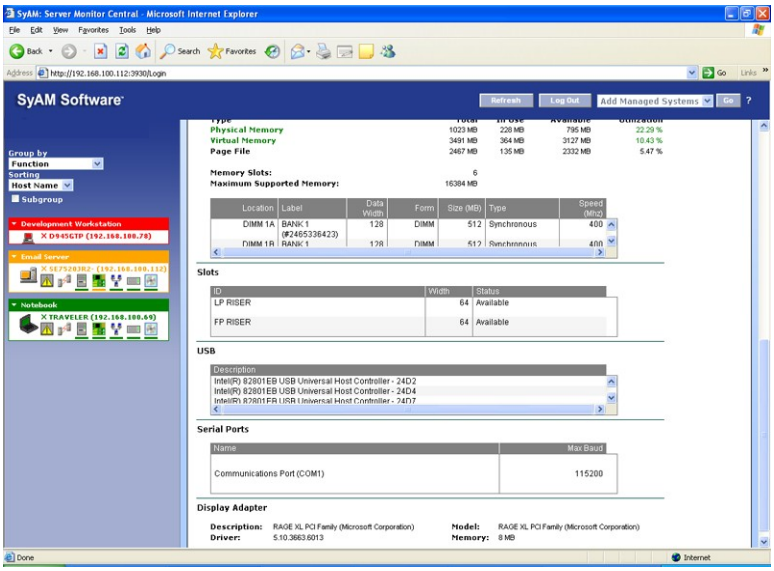


Figure 59: System Detail Tab Continued

Monitoring Memory Errors

SyAM provides real time monitoring and alerting of single- and multi-bit memory errors on systems with supported ECC Memory error monitoring.

The default alerting thresholds are to notify the administrator immediately on a multi-bit error or when two single-bit errors occur within a day.

Through the SyAM System Area Manager Interface the administrator can adjust the thresholds and polling interval periods for both single- and multi-bit errors, and configure their notification methods.

Power Management Tab

The Power Management tab lets the user display and reconfigure the power management policies for the managed system.

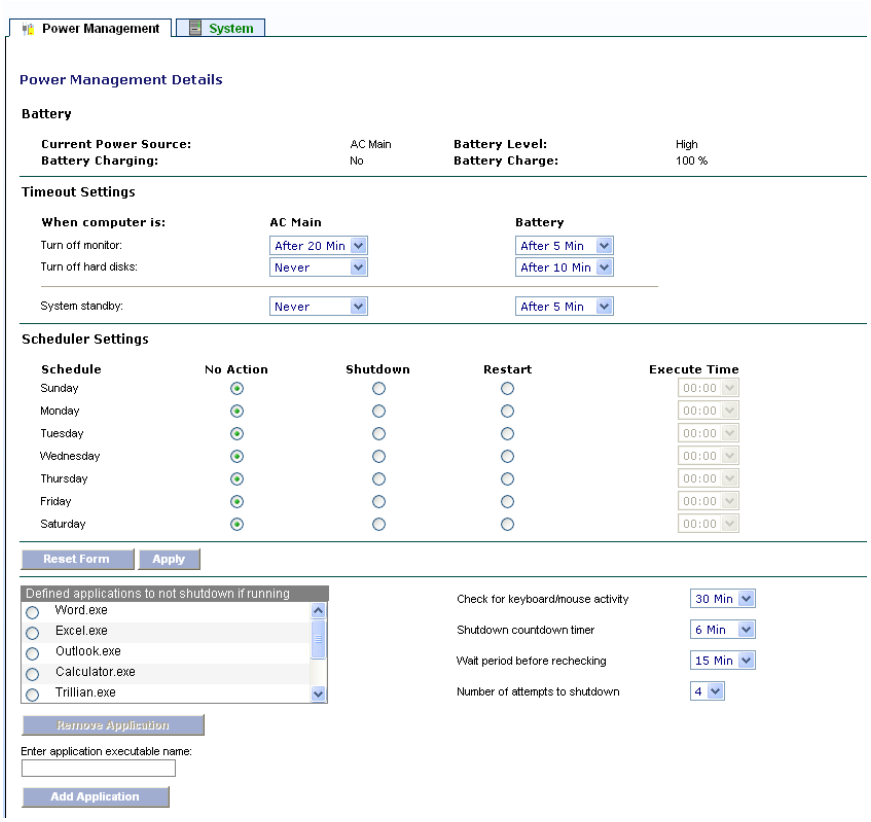


Figure 60: Power Management Tab

Timeout Settings

From here you can configure the power scheme settings for the managed system. If the managed system is a notebook there will be two separate sets of settings: one set that will be applied when connected to AC Power, and the other set for when running on battery.

The options are;

- Turn off monitor
- Turn off hard disks
- System standby
- Hibernate – This will only be displayed if the system has hibernation enabled

Battery

This information is only displayed if the managed system is a notebook.

- Current Power Source – States if the system is plugged in using AC Power Cord or is running from the battery
- Battery Charging – States if the battery is in a charging state.
- Battery Level – Current health state of the battery.
- Battery Charge – The % of the battery life available.

Scheduler Settings

You can configure the managed system to be scheduled to perform a graceful system shutdown or restart at any time for each of the days.

To enable, click on the appropriate radio button for the action to be taken that day. (No Action / Shutdown / Restart). Then set the time using the drop down box.

Different actions can be set at different times for each of the days of the week.

Only one action per day can be scheduled.

Press the Apply Button to save the changes made.

Defined Applications not to shutdown if running

You can enter the name of an application if found to be running it will not perform the scheduled shutdown.

To add an application, Enter the name of the application executable and press the Add Application button.

To remove an application, click on the radio button next to the application you wish to remove and press the Remove Application button.

Check for Keyboard/Mouse Activity

This is the time period that is checked before attempting to perform a scheduled shutdown.

Shutdown Countdown Timer

This is the time period that the user is presented to cancel the scheduled shutdown.

Wait Period before Rechecking

This is the time period that the agent will wait before attempting to perform the scheduled shutdown.

Number of Attempts to Shutdown

This is the number of attempts the agent will attempt to perform the scheduled shutdown for that day.

Hardware Detail Tab

All environmental sensors discovered on your platform are displayed in the Hardware Tab. This includes fans, temperatures, voltages, power redundancy loss and physical security. The number and type of sensors displayed is dependent upon the system platform and its configuration.

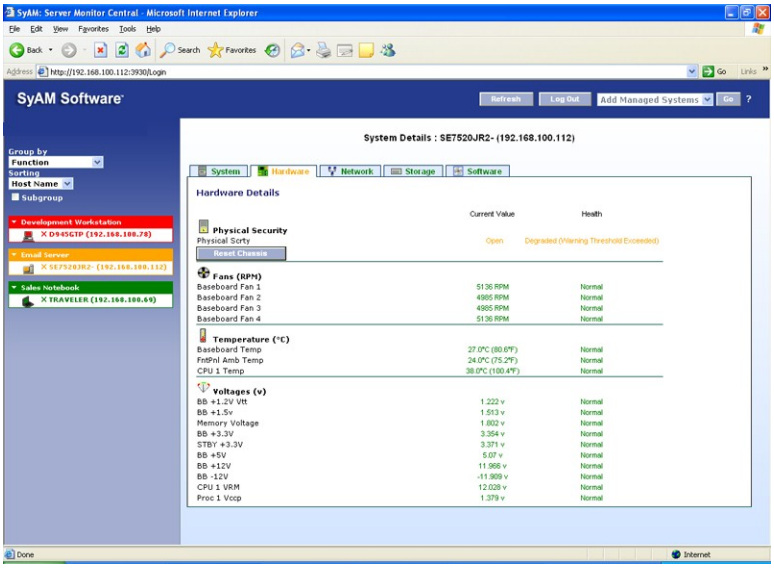


Figure 61: Hardware Detail Tab

Reset Chassis Intrusion

Some hardware platforms that support a chassis intrusion sensor, do not automatically reset the sensor state to normal when the chassis in closed. For such systems the Reset Chassis button causes the platform to reset the state of the sensor to normal.

Network Detail Tab

The Network Tab displays detailed information on adapters connecting the managed system to the network, including adapter and connection speed, connection status, IP address, and MAC address. Additionally the send and receive byte counts and calculated utilization over the last approximately 20 seconds is provided.

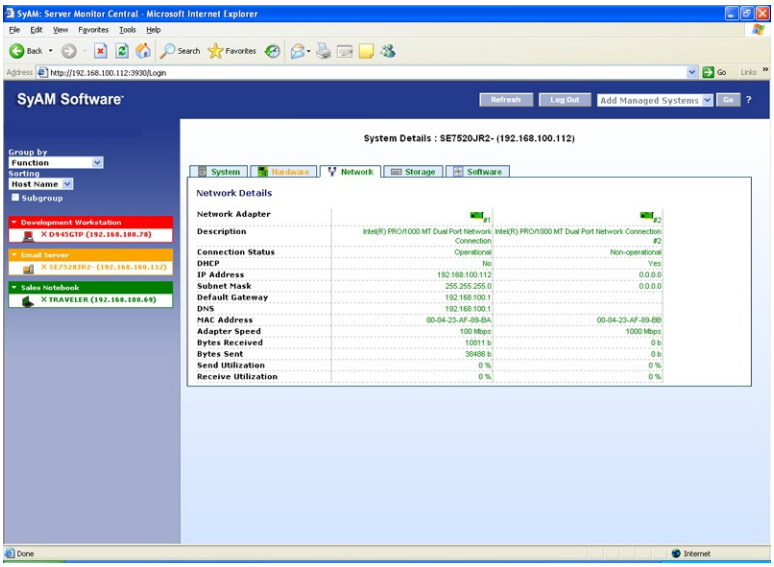


Figure 62: Network Detail Tab

Storage Detail Tab

The Storage Tab displays detailed information on physical and logical disks associated with the system being monitored. Physical disk attributes reported include vendor information, device ID, SCSI ID, and size. Logical disk attributes reported include name, size, space allocation, and utilization.

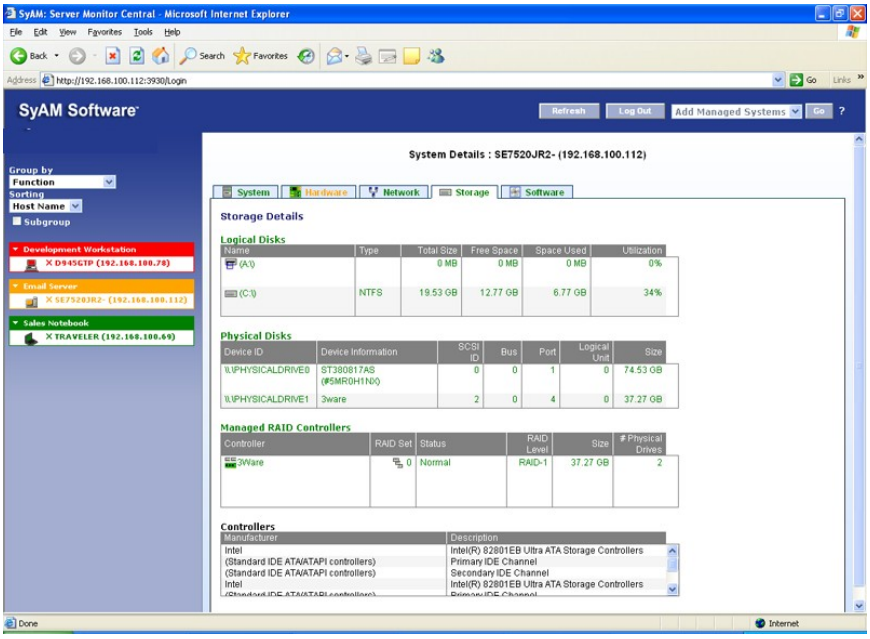


Figure 63: Storage Detail Tab

RAID Management

SyAM System Client – Server and Desktop performs integrated monitoring of PCI RAID Controllers. All discovered PCI RAID Controllers that we support will be monitored, and their summary configuration and status displayed under "Managed RAID Controllers" within the Storage tab.

SyAM System Client – Server and Desktop will discover RAID Controllers that it can manage only if the required RAID drivers are installed. If a new RAID Controller is installed after SyAM System Client – Server and Desktop has been started, then restart the system for it to discover the new Managed RAID Controller.

Please check the release Notes for the list of RAID Controller compatibility for the version of software you are using.

SMART Drive Pre- Failure Monitoring

Directly attached disk drives that are SMART capable are checked daily. Supported disk technologies include P-ATA, S-ATA, SCSI and FC. The administrator can be notified of bad disk drives before they fail and potentially lose data. Notification of a bad SMART status (Pending failure) is done via the notification options configured for the drive.

The Storage Details tab visually shows physical drive status. A physical drive in the warning state (amber colored) is pending failure and has reported a bad SMART status.

RAID Management

Managed PCI RAID controllers can be configured with SyAM System Area Manager - Server. Navigation begins from the Storage Details tab

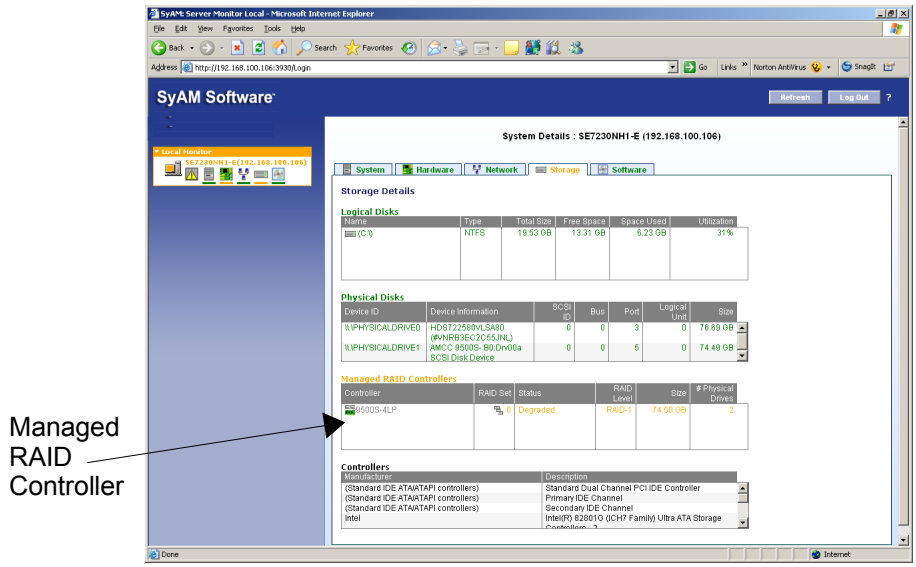


Figure 64: Storage Details – Managed RAID Controllers

Click on the RAID Controller to open up the RAID Controller window.

RAID Controller Details Screen

The RAID Controller screen is divided into 4 parts.

RAID Controller Details – Displays the controller model, firmware version, Cache if present, Number of Bus, ID, BIOS Version, BBU Presence and Max Devices per Buses

RAID Set Details – Displays the current RAID sets configured on this controller, including their description , RAID Set #, and Status (Normal, Init, Rebuild, Degraded, Failed). A RAID Set (also called a RAID Array) appears to the operating system as a physical disk.

Physical Drives – Displays the physical drives connected to the RAID controller, including their location on the BUS, ID, Status, Capacity, Vendor and Model. Physical drives in use by a RAID controller are typically not visible to the operating system.

Available Arrays – Displays the physical arrays defined by the RAID controller. A physical array is a grouping of drives on which RAID Sets are created. The display includes the RAID levels and capacities available for creating additional RAID sets.

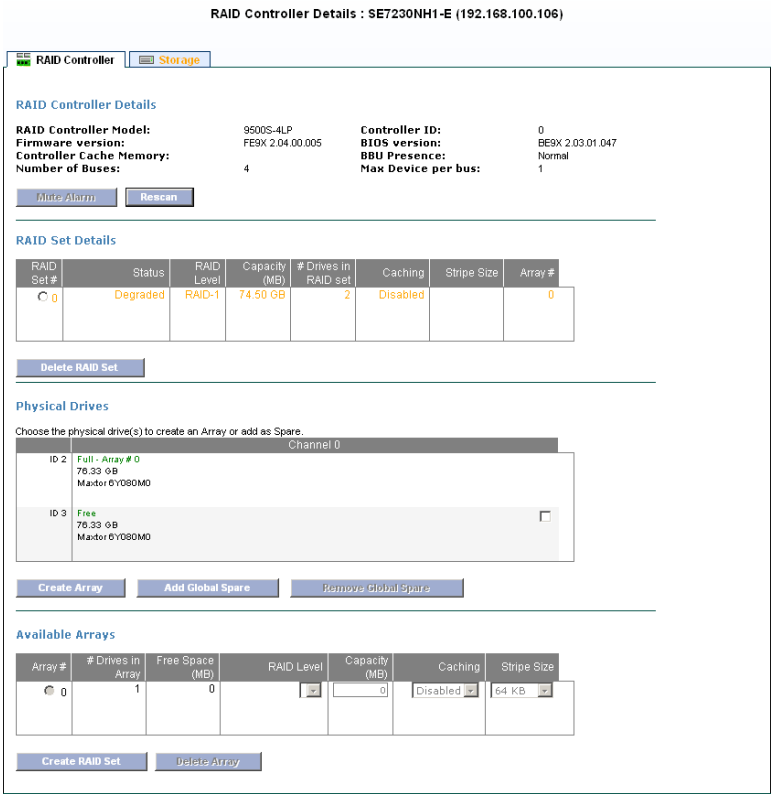


Figure 65: RAID Controller Details Screen

Steps in Creating a RAID Set

1. Decide if you will create a RAID Set on an existing Physical Array, or want to first create a new Physical Array for the RAID Set. If you will use an existing Physical Array proceed to step 4.
2. To create a Physical Array, choose the physical drives that you wish to make up the array by clicking on their check box. (Remember only drives not in use in other arrays or as hot spares can be used.)
3. Click on the Create Array button – wait for the screen to update

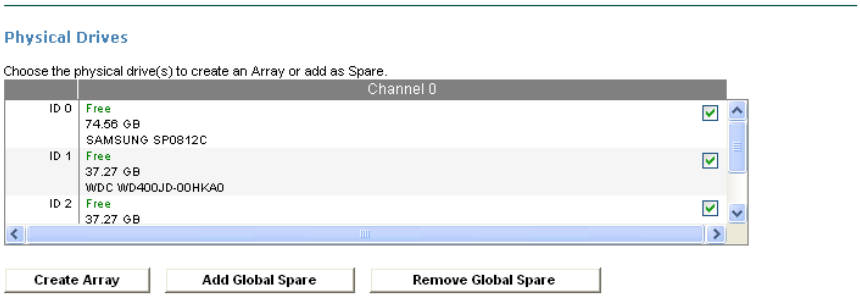


Figure 66: Physical Drives – Choosing drives for the Array

4. Now click on the Physical Array that you wish to create the RAID Set on. (***Physical Arrays with no available capacity* will not display any available RAID Set configurations.)**
5. Choose the RAID level from the drop down box. Only RAID levels supported for the particular set of drives in the Physical Array will be presented. The maximum capacity available for the selected RAID level is calculated and displayed. You may enter a lower capacity to be used for this RAID Set.

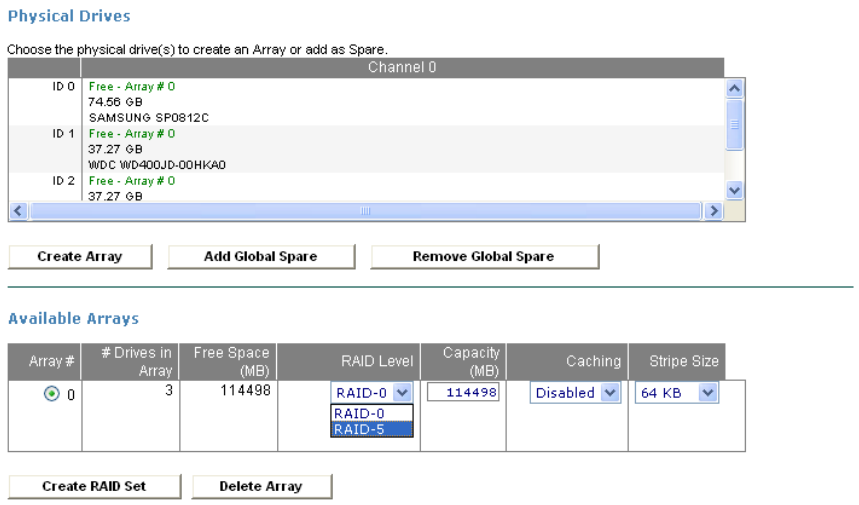


Figure 67: Available Array - Configuring the RAID Set

6. Next choose the Caching policy and stripe size from the drop down boxes.
7. Click the Create RAID Set button to create the RAID Set.
8. The system will now process your configuration and will create the RAID Set. If for any reason the create operation fails, a message will be displayed at the top of the screen explaining the cause for failure.
9. The new RAID Set will now appear under the RAID Set Details
10. If you created a Physical Array in Step 3 and decided not to create a RAID Set on it, you may dismiss it by selecting it and clicking the Delete Array button . You cannot delete Physical Arrays that have RAID Sets created on them.

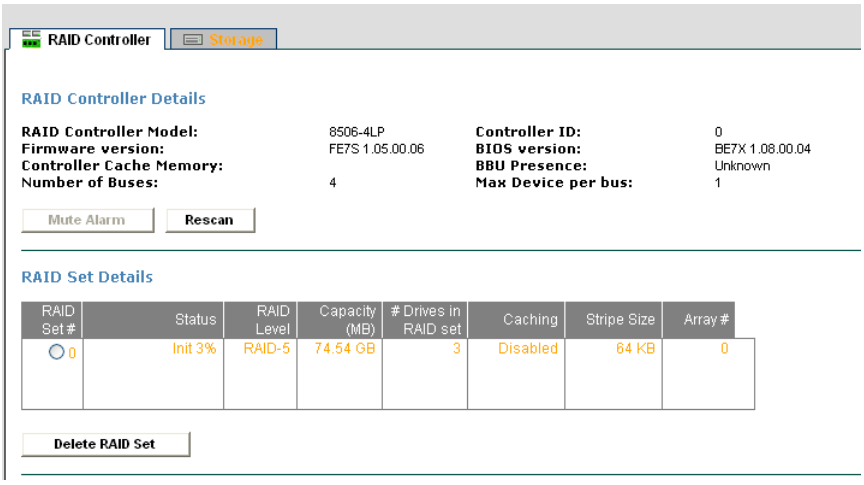


Figure 68: RAID Set Details – Information on Configured RAID Set

Adding/Removing a Global Spare

1. Choose the physical drive that you wish to become a global spare to the RAID Set by clicking on its check box, then click on the Add Global Spare button.
2. To remove a global spare click on the check box next to the drive that is currently displayed as a hot spare, then click the Remove Global Spare button.

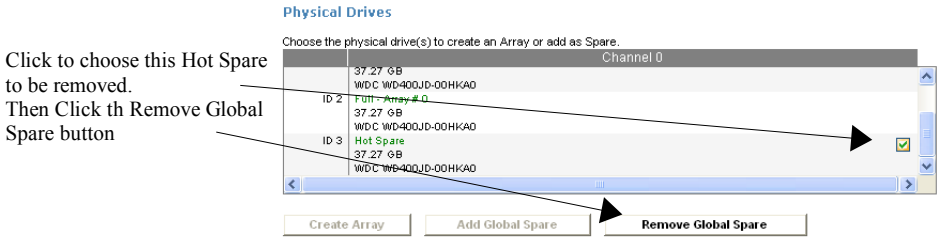


Figure 69: Removing a Hot Spare drive

Deleting a RAID Set

1. *Under RAID Set Details click the radio button next to the RAID Set to delete. Then click on the Delete RAID Set button. Note that when multiple RAID Sets are present on the same Physical Array, only the last RAID Set displays a radio button and may be selected to delete.*

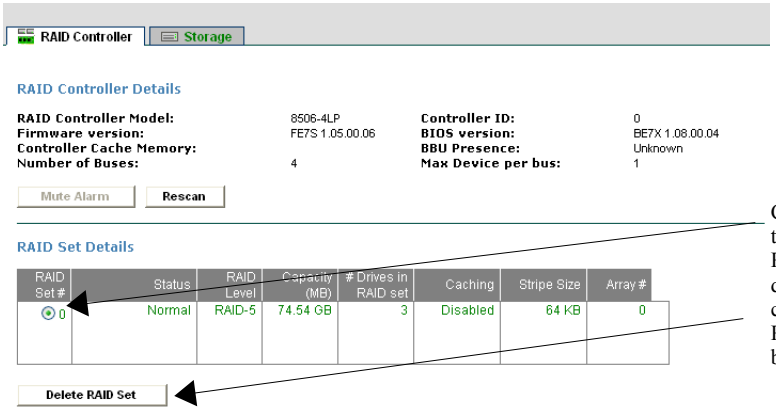


Figure 70: RAID Set Details – Deleting a RAID set

Software Detail Tab

The Software Tab displays detailed information on the processes, services, and applications installed and running on the system being monitored.

End Process – Start/Stop Service

The administrator can stop a running process , and start or stop a service of a managed system, without having to physically visit that system. The startup type and current status of each service is displayed.

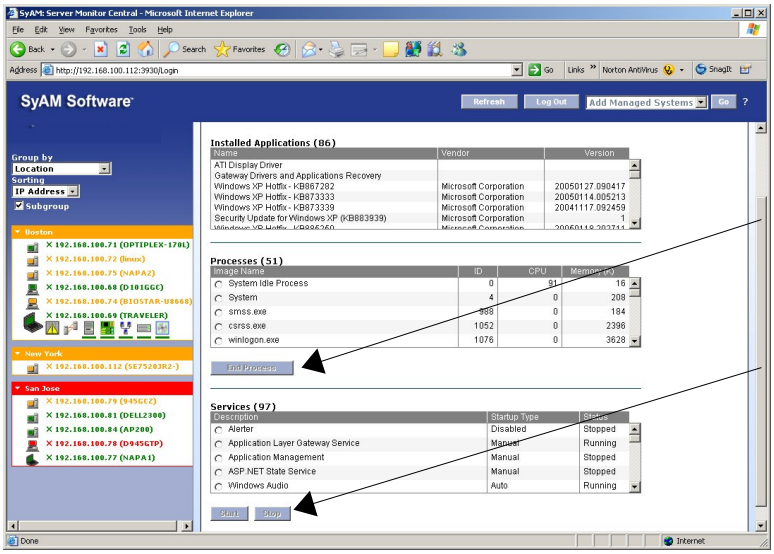


Figure 71: Software Detail Tab

To end a process, chose the process by clicking on the radio button to the left of the Process Name, then click the End Process button .

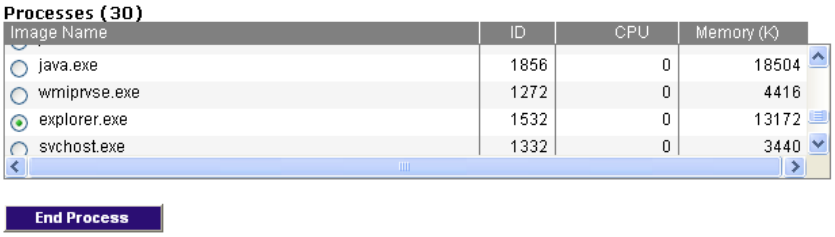


Figure 72: End the Process

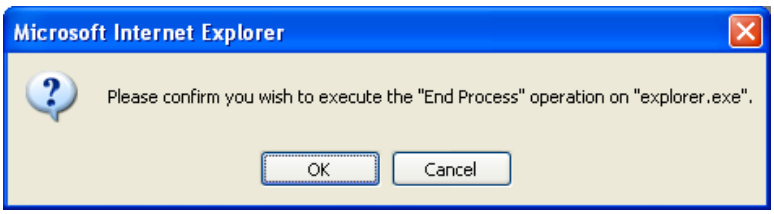


Figure 73: Confirm to End the Process

To Start a Service choose the service by clicking on the radio button to the left of the Service Name, then click on the Start button. The service must be in a stopped state in order to be started.

Figure 74: Starting a Service

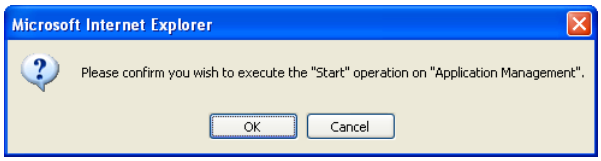

Microsoft Internet Explorer
Please confirm you wish to execute the "Start" operation on "Application Management".
OK
Cancel

Figure 75: Confirm to Start the Service

To Stop a Service choose the service by clicking on the radio button to the left of the Service Name, then click on the Stop button . The service must be in a running state in order to be stopped.

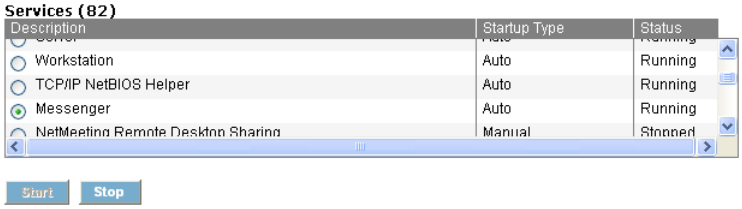


Figure 76: Stopping a Service

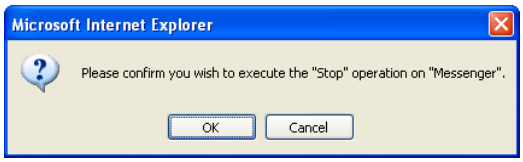


Figure 77: Confirm to Stop the Service

Chapter 10: Configuring Platform Event Trap Support

This chapter provides instruction on how to configure the system running the System Area Manager - Server software to receive Platform Event Traps

Platform Event Traps

System Area Manager is able to receive SNMP alerts in the Platform Event Trap Format (PETs).

The Baseboard Management Controller (BMC) that performs the IPMI management is able to issue SNMP traps when a physical sensor event occurs. The SNMP Trap is formatted to a Platform Event Trap (PET) standard. System Area Managerl is able to capture these PET's and notify the central administrators via a chosen notification method designated in the Central Alert Matrix. System Area Manager converts the SNMP trap information into a simple description of the event, providing the administrator with information to identify which server sent the event, as well as the type and severity of the event.

In addition to being notified about the PET, System Area Manager stores the complete SNMP Trap information within its Event Log for later review.

-----Original Message-----
From: SystemAreaManager@8GM.com
[mailto:System Area Manager@8GM.com]
Sent: Sunday, December 28, 2003 3:44 PM
To: John.Doe@company.com
Subject: System Area Manager Alert

Voltage Over Max Threshold Alert from 192.168.200.199 at Sun Dec 28

Figure 78: Example of a PET email alert

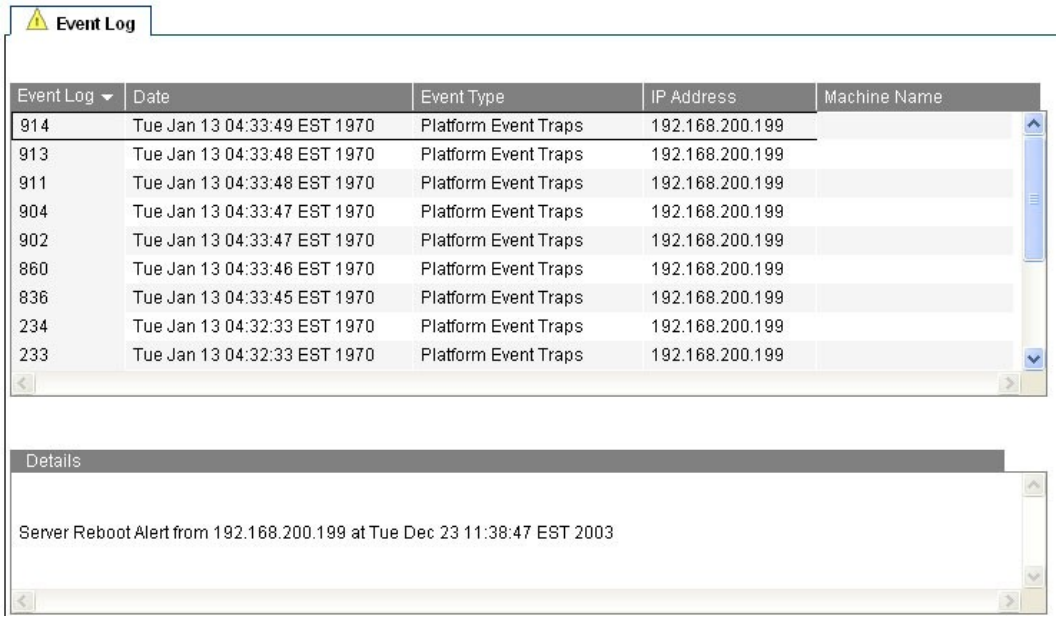

Event Log
Event Log
Date
Event Type
IP Address
Machine Name
914 Tue Jan 13 04:33:49 EST 1970 Platform Event Traps 192.168.200.199
913 Tue Jan 13 04:33:48 EST 1970 Platform Event Traps 192.168.200.199
911 Tue Jan 13 04:33:48 EST 1970 Platform Event Traps 192.168.200.199
904 Tue Jan 13 04:33:47 EST 1970 Platform Event Traps 192.168.200.199
902 Tue Jan 13 04:33:47 EST 1970 Platform Event Traps 192.168.200.199
860 Tue Jan 13 04:33:46 EST 1970 Platform Event Traps 192.168.200.199
836 Tue Jan 13 04:33:45 EST 1970 Platform Event Traps 192.168.200.199
234 Tue Jan 13 04:32:33 EST 1970 Platform Event Traps 192.168.200.199
233 Tue Jan 13 04:32:33 EST 1970 Platform Event Traps 192.168.200.199
Details
Server Reboot Alert from 192.168.200.199 at Tue Dec 23 11:38:47 EST 2003

Figure 79: Example of PET information in the Event Log

PET Sensor Types Supported:

-Temperature
-Voltage
-Current
-Fan
-Physical Security
-Platform Security
-Processor
-Power Supply
-Power Unit
-Cooling Devices
-Memory
-Boot Error
-OS Critical Stop

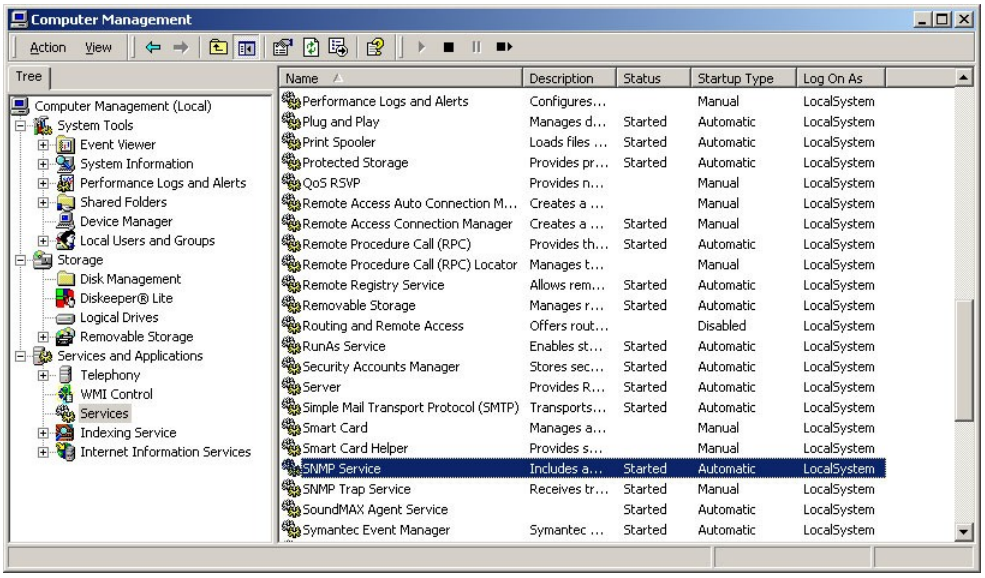
Note: If the PET received is not recognized, the administrator will be notified that an unidentified PET has been received and the Trap detail will be stored in the event log.
For more information on PET 1.0 specification please refer to the DMTF Website.

Configuring System Area Manager to Receive Platform Event Traps

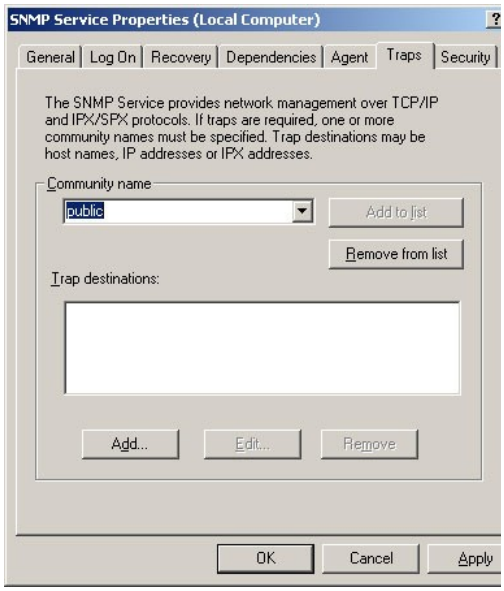
In order for System Area Manager to receive and process PETS, the system must have its SNMP service properties changed to include the community name “Public” and that no other SNMP Trap service is running, including the SNMP Trap Service that is automatically installed with the Windows SNMP Option.

To configure the SNMP Service Properties:

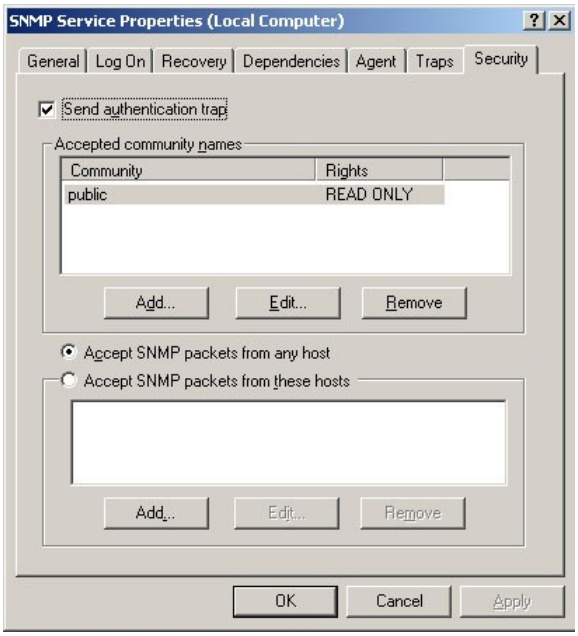
1. Open “Computer Management”
2. Under Services and Applications, select SNMP


Computer Management
Action View
Tree
Computer Management (Local)
System Tools
Event Viewer
System Information
Performance Logs and Alerts
Shared Folders
Device Manager
Local Users and Groups
Storage
Disk Management
Diskeeper® Lite
Logical Drives
Removable Storage
Services and Applications
Telephony
WMI Control
Services
Indexing Service
Internet Information Services
Name
Description
Status
Startup Type
Log On As
Performance Logs and Alerts Configures... Manual LocalSystem
Plug and Play Manages d... Started Automatic LocalSystem
Print Spooler Loads files ... Started Automatic LocalSystem
Protected Storage Provides pr... Started Automatic LocalSystem
QoS RSVP Provides n... Manual LocalSystem
Remote Access Auto Connection M... Creates a ... Manual LocalSystem
Remote Access Connection Manager Creates a ... Started Manual LocalSystem
Remote Procedure Call (RPC) Provides th... Started Automatic LocalSystem
Remote Procedure Call (RPC) Locator Manages t... Manual LocalSystem
Remote Registry Service Allows rem... Started Automatic LocalSystem
Removable Storage Manages r... Started Automatic LocalSystem
Routing and Remote Access Offers rout... Disabled LocalSystem
RunAs Service Enables st... Started Automatic LocalSystem
Security Accounts Manager Stores sec... Started Automatic LocalSystem
Server Provides R... Started Automatic LocalSystem
Simple Mail Transport Protocol (SMTP) Transports... Started Automatic LocalSystem
Smart Card Manages a... Manual LocalSystem
Smart Card Helper Provides s... Manual LocalSystem
SNMP Service Includes a... Started Automatic LocalSystem
SNMP Trap Service Receives tr... Started Manual LocalSystem
SoundMAX Agent Service Started Automatic LocalSystem
Symantec Event Manager Symantec ... Started Automatic LocalSystem

3. Under the SNMP Services General Properties, Select Public as the community name and click <Apply>.



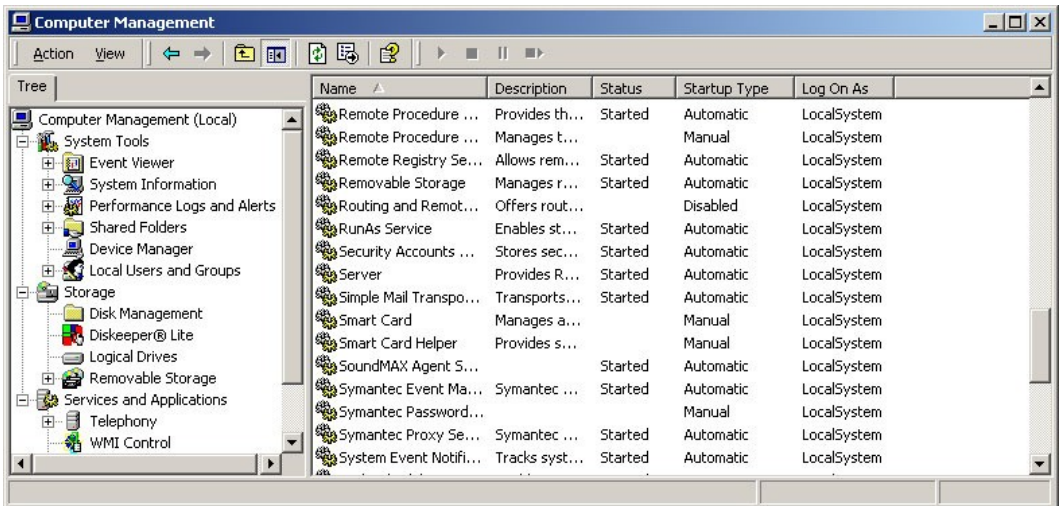
4. Under the SNMP Services Security properties, click the check box to enable Accept SNMP packets from any Host, or enter the IP addresses configured for the BMC on the IPMI-enabled servers.



5. Press the OK button and close the services window.

6. You will need to reboot the system in order for these changes to take effect.

If you cannot find the SNMP service, it means that it is not loaded.


Computer Management
Action View
Tree
Computer Management (Local)
System Tools
Event Viewer
System Information
Performance Logs and Alerts
Shared Folders
Device Manager
Local Users and Groups
Storage
Disk Management
Diskeeper® Lite
Logical Drives
Removable Storage
Services and Applications
Telephony
WMI Control
Name
Description
Status
Startup Type
Log On As
Remote Procedure ... Provides th... Started Automatic LocalSystem
Remote Procedure ... Manages t... Manual LocalSystem
Remote Registry Se... Allows rem... Started Automatic LocalSystem
Removable Storage Manages r... Started Automatic LocalSystem
Routing and Remot... Offers rout... Disabled LocalSystem
RunAs Service Enables st... Started Automatic LocalSystem
Security Accounts ... Stores sec... Started Automatic LocalSystem
Server Provides R... Started Automatic LocalSystem
Simple Mail Transpo... Transports... Started Automatic LocalSystem
Smart Card Manages a... Manual LocalSystem
Smart Card Helper Provides s... Manual LocalSystem
SoundMAX Agent S... Started Automatic LocalSystem
Symantec Event Ma... Symantec ... Started Automatic LocalSystem
Symantec Password... Manual LocalSystem
Symantec Proxy Se... Symantec ... Started Automatic LocalSystem
System Event Notifi... Tracks syst... Started Automatic LocalSystem

To load the SNMP service:

1. Open up Control Panel, Add/Remove Programs and choose the <Add/Remove Windows Components> button on the left side of the screen.

2. Scroll down the list until you find Management and Monitoring Tools, and double click to display the options.

3. Once the options are shown, click on the check box next to Simple Networking Protocol, and click <OK>.

4. Click on the next button. This will then start to load the windows SNMP component. If the files are not found on the server's disks it will prompt you to insert the Windows Server OS CD's.

5. Once installed you follow the instructions on how to configure the SNMP service.

If another SNMP service is already running then the System Area Manager PET trap listener service will not be able to start. You will receive a notification and the event will be recorded in the event log.

Also the Central Alert Matrix will inform you that the Platform Event Trap Listener service is not running.

Chapter 11: Database Backup/Restore

This chapter contains information to explain how to backup and restore the System Area Manager database.

Backing Up the Database

As the System Area Manager stores the System Details and events of the managed systems in its database we recommend that once a month you back up the database.

To perform the backup, choose the Database Backup option from the Program Menu

<SyAM>
    <Utilities>
        <Database Backup>
        <Database Restore>

Enter the backup file name you wish to use
example: SyAM-Backup-Jan30

This will backup the data to the folder using the file name you entered
\SyAM\javadb\Database_Backups\SyAM-Backup-Jan30

We recommend that you copy this folder to a location off of the system running the System Area Manager, so in the event that the system drive fails you will be able to restore the System Area Manager backup.

Restoring the Database

In the event that you need to restore a Database backup for the System Area Manager system details and event log you can do this at any time.

To restore the database backup, first copy the backup folder to the \SyAM\javdb\Database_Backups\ folder, then choose the Database Restore option from the Program Menu

example: \SyAM\javadb\Database_Backups\SyAM-Backup-Jan30

<SyAM>
    <Utilities>
        <Database Backup>
        <Database Restore>

Enter the backup name you wish to restore
example: SyAM-Backup-Jan30

Restoring the database will restore the Management Tree, System Details and Events in the Event log to the stage the backup was made.

In the event system clients that were reporting to the System Area Manager at the time the backup was made, but are no longer reporting to the System Area Manager they will be restored but will appear grey (Unknown) in the tree. Click on the X next to their name to remove them from the management tree.

Chapter 12: Contact Details & Glossary

This chapter contains technical support contact information as well as a glossary.

Contact Details

Contact	product-support@syamsoftware.com
Web	www.syamsoftware.com
Support Information	http://www.syamsoftware.com/
Product Information	http://www.syamsoftware.com/

Glossary

Adding a sensor to the alert matrix

Sensors are automatically monitored, they have their sensor category default notifications applied to them.

Asset-monitoring event

Discrepancy in the systems physical and software inventory.

Central Alert Matrix

Administrators use this screen to define the notifications for all of the managed systems.

Central Alert Notification Settings

Notification and configuration details for the Central Alert matrix.

Central Management Tree

Displays in a tree format all of the managed systems.

Changing Central Management Tree grouping

Click on the <Group By> drop down menu to group systems by Location, Function, or Operating System.

Changing Central Management Tree sorting order

Click on the <Sort By> drop down menu to sort by IP address or Machine Name.

Changing to which System Area Manager the system reports

Remove the system from the first System Area Manager tree to stop the system from reporting. Once this is done, add the system to the second System Area Manager tree by following the instructions “Add Managed System”

Critical Level

The level of the threshold which is operating beyond the normal and warning thresholds.

Current Value

The actual reported sensor reading for the system component on a timed reporting cycle.

Email #1/ #2

Primary and secondary administrator email addresses

Event Log

Record of all of the managed systems events.

From Address

Administrators can define a unique name for the SyAM alerting email address.

Graceful shutdown

Shutdown a managed system remotely if the agent on that system is in a functioning state.

Grouping systems

Group managed system by location, operating system, or function.

Hardware Detail Screen

Information on the system components being monitored, including fans, temperature, voltages, etc.

Hardware Event

When a threshold is met or exceeded by a physical component of the system.

Header Bar

The header bar within this browser contains the **<Logout> <Refresh> <?>** function buttons

Health colors

Green = Fully Functional
Amber = Warning threshold exceeded
Red = Critical Threshold exceeded
Grey = System update pending
Blue = Agent has been manually stopped
Purple = System is no longer responding
Black = System has been shut down
Cyan = System has expired Central Management License Key

Intervals

Readings on all monitored systems and components are at preset cycles of 20 seconds.

IPMI Event Log

Hardware event log stored within the IPMI based server

Logical Sensor

Storage, network adapters, removable disk drives, and CPU and memory usage.

Login

Administrators must login using a user name and password that has administrative rights to the machine that is running SyAM software

Lower threshold

The lowest threshold to be alerted upon if it is exceeded.

Network Detail Screen

Information on network adapters and their configuration.

Network Event

Network connectivity is lost.

Notification Settings

Email, SMS/pager, System Area Manager, Network Messages and SNMP Traps.

Performance utilization event

CPU or memory utilization threshold is met or exceeded.

Physical Sensors

Physical Security, Fans, Temperature, Voltages and Power Unit sensor monitored

Platform Event Trap (PET)

SNMP formatted trap received from IPMI-enabled server

Remote Management

Shutdown, Reset, Wake on LAN and Remote Console

Remote Console

The Remote Console provides the capability of taking control of a managed systems local screen, keyboard and mouse directly through the web browser from the System Area Manager Interface.

Removing a sensor from the System Alert matrix

To remove a sensor it must be in a critical state, then click on the “X” to permanently delete this sensor from the alert matrix.

Removing systems from System Area ManagerTree

To remove a system from the System Area Manager Tree, select the system and click on the X.

Reset period

The frequency of notifications sent after the initial alert has been sent and if the sensor has not been corrected.

Restore Physical Sensor Thresholds

This will reset to the original sensor threshold values when you click on this button.

Sample period

Time that is used to take CPU and Memory utilization samples.

Sensor Status Change back to normal

When a sensor returns back to within its operating threshold range.

SyAM Agent

Non-intrusive monitoring agent configured and managed by the SyAM System Area Manager

SyAM System Area Manager

Provides monitoring and communications with all managed agents

SyAM System Client

Non-intrusive monitoring agent that can be browsed to directly or managed and configured from the SyAM System Area Manager

SyAM System Client Tree

Browsing directly to a system running SyAM System Client.

SMS Pager #1/#2

Primary and secondary administrator SMS/Pager addresses.

SMTP address

Mail system address: example: mail.company.com or 192.168.1.100

SNMP Traps

Notification from a System Client or System Area Manager to an enterprise framework server – Requires System Area Management (SyAM) MIB to be installed on enterprise framework server.

Software Detail Screen

Information on the processes, services, and applications installed.

Storage Detail Screen

Information on physical and logical disks, controllers and removable devices.

Storage Event

Logical disk has reached its utilization threshold, Loss of logical disk, or Loss of Physical disk.

System Absent

When the System Area Manager is no longer able to communicate with a managed system, it is reported as being absent, unless it was correctly shutdown.

System Alert Matrix

Interface to configure sensor thresholds and notification options.

System Alert Notification Settings

Notification and configuration details for the System Alert matrix.

System Detail Screen

Information on the system's configuration, BIOS, operating system, location, memory, CPU, etc.

Upper Threshold

The highest threshold to be alerted upon if exceeded.

User name and Password for outgoing Authentication

Enter the administrator user name and password (if the outgoing email system requires authentication)

Wake on LAN

Power up a WOL-enabled managed system.

Warning Level

The level of the threshold that is operating between the normal and critical thresholds.

Welcome

Displays the Revision and contact details for the product.